opentext™

OpenText™ Directory and Resource Administrator

Use

Version : 10.3
PDF Generated on : 15/09/2025

Table of Contents

1. Use

The *User Guide* provides conceptual information about the OpenText Directory and Resource Administrator (DRA) product. This book defines terminology and various related concepts.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

Additional Documentation

This guide is part of the Directory and Resource Administrator documentation set. For the most recent version of this guide and other DRA documentation resources, visit the DRA Documentation site.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the **comment on this topic** link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care at https://www.microfocus.com/support-and-services/.

1.1. Getting started

Before you begin managing Active Directory objects using the OpenText Directory and Resource Administrator (DRA) you should understand the basic tenets of what DRA will do for your enterprise and the role of DRA components in the product architecture.

- What is Directory and Resource Administrator

- Understanding Directory and Administrator Components

1.1.1. What is OpenText Directory and Resource Administrator

Directory and Resource Administrator delivers secure and efficient privileged-identity administration of Microsoft Active Directory (AD). DRA performs granular delegation of "least privilege" so that administrators and users receive just the permissions needed to complete their specific responsibilities. DRA also enforces adherence to policy, provides detailed-activity auditing and reporting, and simplifies repetitive task completion with IT process automation. Each of these capabilities contributes to protecting your customers' AD and Exchange environments from the risk of privilege escalation, errors, malicious activity, and regulatory non-compliance, while reducing administrator burden by granting self-service capabilities to users, business managers, and Help Desk personnel.

DRA also extends the powerful features of Microsoft Exchange to provide seamless management of Exchange objects. Through a single, common user interface, DRA delivers policy-based administration for the management of mailboxes, public folders, and distribution lists across your Microsoft Exchange environment.

DRA provides the solutions you need to control and manage your Active Directory, Microsoft Windows, Microsoft Exchange, and Entra ID Active Directory environments.

- **Support for Entra ID and on-premises Active Directory, Exchange, and Skype for Business:** Delivers administrative management of Entra ID and on-premises Active Directory, on-premises Exchange Server, on-premises Skype for Business, Exchange Online, and Skype for Business Online.

- **Granular user and administrative privilege-access controls:** Patented ActiveView technology delegates just the privileges needed to complete specific responsibilities and protect against privilege escalation.

- **Customizable web console:** Intuitive approach enables non-technical personnel to easily and safely perform administrative tasks via limited (and assigned) capabilities and access.

- **In-depth activity auditing and reporting:** Provides a comprehensive audit record of all activity performed with the product. Securely stores long-term data and demonstrates to auditors (e.g. PCI DSS, FISMA, HIPAA and NERC CIP) that processes are in place for controlling access to AD.

- **IT Process Automation:** Automates workflows for a variety of tasks, like provisioning and deprovisioning, user and mailbox actions, policy enforcement, and controlled self-service tasks; increases business efficiencies, and reduces manual and repetitive administrative efforts.

- **Operational integrity:** Prevents malicious or incorrect changes that affect the performance and availability of systems and services by providing granular access control for administrators and managing access to systems and resources.

- **Process enforcement:** Maintains the integrity of key change management processes that help you improve productivity, reduce errors, save time, and increase administration efficiency.

- **Integration with Change Guardian:** Enhances auditing for events generated in Active Directory outside of DRA and workflow automation.

1.1.2. Understanding OpenText Directory and Resource Administrator Components

The components of DRA that are consistently used to manage privileged access include primary and secondary servers, administrator consoles, reporting components, and the Workflow Engine to automate workflow processes.

The following table identifies the typical user interfaces and Administration servers used by each type of DRA user:

Type of DRA User	User Interfaces	Administration Server
DRA Administrator (The person who will maintain the product configuration)	Delegation and Configuration Console	Primary server
Advanced Administrator	DRA Reporting PowerShell CLI DRA ADSI Provider	Any DRA server
Help Desk Occasional Administrator	Account and Resource Management node in the Delegation and Configuration Console Web Console	Any DRA server

DRA Administration Server

The DRA Administration server stores configuration data (environmental, delegated access, and policy), executes operator and automation tasks, and audits system-wide activity. While supporting several console and API level clients, the server is designed to provide high availability for both redundancy and geographic isolation through a Multi-Master Set (MMS) scale-out model. In this model, every DRA environment will require one primary DRA Administration server that will synchronize with a number of additional secondary DRA Administration servers.

We strongly recommend that you do not install Administration servers on Active Directory domain controllers. For each domain that DRA manages, ensure there is at least one domain controller in the same site as the Administration server. By default, the Administration server accesses the closest domain controller for all read and write operations; when performing site-specific tasks, such as password resets, you can specify a site specific domain controller to process the operation. As a best practice, consider dedicating a secondary Administration server for your reporting, batch processing, and automated workloads.

Account and Resource Management

Account and Resource Management is a node in the Delegation and Configuration Console for DRA assistant administrators to view and manage delegated objects of connected domains and services.

Web Console

The Web Console is a web-based user interface that provides quick and easy access to DRA assistant administrators to view and manage delegated objects of connected domains and services.

Administrators can customize the look and use of the Web Console to include customized enterprise branding and customized object properties, as well as configure integration with Change Guardian servers to enable change auditing that occurs outside of DRA.

The DRA Administrator can also create and modify automated workflow forms to run routine automated tasks when triggered.

Unified Change History is another feature of the Web Console that enables integration with Change History servers to audit changes made to AD objects outside of DRA. Change History report options include the following:

- Changes made to...

- Changes made by...

- Mailbox created by...

- User, group, and contact email address created by...

- User, group, and contact email address deleted by...

- Virtual attribute created by...

- Objects moved by...

Reporting Components

DRA Reporting provides built-in, customizable templates for DRA management and details of DRA managed domains and systems:

- Resources reports for AD objects

- AD object data reports

- AD summary reports

- DRA configuration reports

- Exchange configuration reports

- Office 365 Exchange Online reports

- Detailed activity trends reports (By month, domain, and peak)

- Summarized DRA activity reports

DRA reports can be scheduled and published through SQL Server Reporting Services for convenient distribution to stakeholders.

Workflow Engine

DRA integrates with the Workflow Engine to automate workflow tasks via the Web Console where assistant administrators can configure the Workflow Server and execute customized workflow automation forms, and then view the status of those workflows. For more information about the Workflow Engine, see Workflow Automation documentation on the DRA Documentation site.

Product Architecture

On-Premises Network

DRA Server

Web Server(IIS)

Reporting

Workflow Engine

Primary Site

Primary Site
- Mail Server
- Public Folders

Active Directory
- Managed Domain
- Trusted Domain

Managed Services
- Skype for Business

Managed Resources
- Computers
- Printers

DRA Administration Server
- Primary/Secondary (Hi-Availability)
- Hosted Website
- Reporting
- Workflow Engine

DRA Clients
- Web Console
- Delegation and Configuration Console
- PowerShell command line
- REST Client

Slow Link

Remote Site

Remote Environment
- Active Directory
- Exchange
- Managed Services
- Managed Resources

Remote DRA Environment
- DRA Secondary Administration Servers
- DRA Clients

Azure

Office 365
- Exchange Online
- Licensing

Active Directory
- Azure Managed Tenant

1.2. Working with the user interfaces

DRA user interfaces address a variety of administration needs. These interfaces include:

Web Console

> Enables you to perform common account and resource administration tasks through a Web-based interface. You can access the Web Console from any computer running Internet Explorer, Chrome, or Firefox.

PowerShell

> The PowerShell module allows non-DRA clients to request DRA operations using PowerShell cmdlets.

NetIQ Reporting Center Console

> Enables you to view and deploy Management reports so you can audit your enterprise security and track administration activities. Management reports include activity reports, configuration reports, and summarization reports. Many of these reports can be viewed in a graphical representation.

1.2.1. Web Console

The Web Console is a Web-based user interface that provides quick and easy access to many user account, group, computer, resource, and Microsoft Exchange mailbox tasks. You can customize object properties to increase efficiency of routine tasks. You can also manage general properties of your own user account, such as the street address or cell phone number.

The Web Console displays a task only if you have the power to perform that task.

- Starting the Web Console

- Configuring the Web Console

- Customizing the Web Console

- Managing Objects in the Web Console

- Generating Change History Reports

- Using Workflow Automation

Starting the Web Console

You can start the Web Console from any computer running Internet Explorer. To start the Web Console, specify the appropriate URL in your Web browser address field. For example, if you installed the Web component on the HOUserver computer, type `https://HOUserver.entDomain.com/draclient` in the address field of your Web browser.

> **Note**
>
> To display the most current account and Microsoft Exchange information in the Web Console, set your Web browser to check for newer versions of cached pages at every visit.

DRA Server Connection

You can use one of the three option to log in to the Web Console. The behavior for each option, when logging in, is described in the following table:

Login Screen - Options	Connection Option Descriptions
Use automatic discovery	Finds a DRA server automatically; no configuration options are available
Connect to the default DRA server	The pre-configured server and port details are used. **Note** This option is displayed only when you have configured the default DRA server in the Web Console. Also, if you specify that the client must always connect to the default DRA server, you can view only the **Connect to the default DRA server** option on the login screen.
Connect to a specific DRA server	The user configures the server and port
Connect to a DRA server that manages a specific domain	The user provides a managed domain and chooses a connection option: • Use automatic discovery (in the domain provided) • Primary server for this domain • Search for a DRA server (in the domain provided)

Configuring the Web Console

If you have DRA Administration powers, you can configure Advanced Authentication, client branding and session settings, and all the required server connections for the Web Console. To access any of these settings, log in to the Web Console and navigate to **Administration** > **Configuration**.

Note

The **Administration** tab in the masthead will not display if you do not have the required administrative powers.

- [Advanced Authentication](#)

- [Web Console Branding](#)

- [Client Session Settings](#)

- [Server Connection](#)

Advanced Authentication

Advanced Authentication lets you move beyond a simple user name and password to a more secure way of protecting sensitive information by using multi-factor authentication. Multi-factor authentication is a method of computer access control that requires more than one method of authentication from separate categories of credentials to verify a user's identity.

After the DRA Administrator configures chains and events, if you have the required powers, you can log into the Web Console and enable Advanced Authentication. Once authentication is enabled, every user will be required to authenticate through Advanced Authentication before being given access to the Web Console.

To enable Advanced Authentication, select **Advanced Authentication** from the Configuration tab, click **Enable Advanced Authentication,** and configure the form according to the instructions provided for each field.

For more information about Advanced Authentication, see "[Authentication](#)" in the DRA Administrator Guide.

Web Console Branding

You can customize the login screen and the masthead of the DRA Web Console, as follows:

- **Masthead:** This is the high-level navigation bar at the top of the Web Console after logging in.

  - *Logo image or alternate text:* Displays on the far left of the masthead bar. You can display a logo image or alternate text, but not both.

  - *Masthead color:* Overlays the entire masthead with this color, except for the logo image area.

- **Themed login screen:** How the login page appears when accessing the Web Console URL in your browser. The DRA theme is configured and enabled by default.

  - *Logo image or alternate text:* Displays above the product title and credential fields. You can display a logo image or alternate text, but not both.

  - *Application title:* Displays between the credential fields and logo image.

  - *Notification modal:* This is a message box that overlays and obscures the login

page until the user clicks **OK**. It is typically used to inform the user that access to the console implies consent to follow a company security policy. Once enabled, all users who access the Web Console will get the prompt.

Configure the Masthead

To configure the masthead:

1. Log in to Web Console, and navigate to **Administration** > **Configuration** > **Branding**.

2. Do one of the following. If you add both text and an image file, only the image will be displayed.

   - Update the Logo Image:

     1. Add the saved image file name, including the file extension in the Logo Image field of the **Masthead** tile.

     2. Save the logo image in the "`assets`" directory on the web server. For example:

        `C:\inetpub\wwwroot\DRAClient\assets`

        The optimal image size is 56x56 pixels.

   - Type or overwrite existing text in the Logo Image Alternate Text field of the **Masthead** tile, as required.

3. Click **Save** at the bottom of the page to complete the configuration changes.

Configure the Login Screen

The procedure below provides information for modifying all three configurable options, the company logo, application title, and notification modal. You can modify one, two, or all three of these options.

To change the default theme in the Login screen:

1. Save your company logo in the "`assets`" folder on the web server. For example:

   `C:\inetpub\wwwroot\DRAClient\assets`

   The optimal image size is 115x28 pixels.

2. Log in to Web Console, and navigate to **Administration** > **Configuration** > **Branding**.

3. Replace the file name in the Company Logo Image field of the **Login** tile with the name of the saved image file, including the file extension.

4. Modify the text in the **Application Title** field, as applicable.

5. Click **Show a notification modal at login** to enable this setting, and type a title for the notification prompt. Type or paste the content of the message you want the users to see in the **Content** field. For example:

   You are logging into a secure network. By logging into this system you consent to abide by the company's security policies for network access.

6. Select the style for the message. The style changes the image flag that is attached to the message box (shown below). If desired, you can click Preview to see how the message will be displayed.

💡	Information	⚠	Error
⚠	Warning	❓	Question

7. Click **Save** at the bottom of the page to complete the configuration changes.

Client Session Settings

In Client Session Settings, you can define a time increment for the Web Console to log out automatically after inactivity or set it to never log out automatically.

To configure Auto Logout in the Web Console, navigate to **Administration** > **Configuration** > **Client Session Settings**. Enable the automatic logout feature with the toggle switch and if needed, modify the setting for the inactivity duration, in minutes.

Server Connection

When accessing the login page for the Web Console in your browser, there are **Options** settings that you can configure to define how you connect to DRA. These settings are also located via the **Server Connection** option in the user profile menu of the Web Console. The service port for the DRA Server has the default setting of 8775. You can set a new default for the DRA Server in the user profile or login screen Options when no default is enabled. The connection settings for the Server Connection configuration are retained with your Windows user profile.

Information about the settings you can modify from the **Server Connection** configuration, either from the Options menu on the login screen or the user profile menu after logging in, is provided below:

DRA Server Settings	Description
Use automatic discovery	Finds a DRA server automatically; no configuration options are available
Connect to the default DRA Server (Only displayed if the default is enabled in the Server Connection configuration)	Uses the default setting from the Server Connection configuration (when enabled); no configuration options are available
Connect to a specific DRA server	The user configures the server and port

If desired, you can configure a default location, server and domain, for the DRA Server from the **Server Connection** configuration in the Web Console.

To enable default settings, log in to the Web Console and navigate to **Administration** > **Configuration** > **DRA Server Connection**. Enable the connection settings that you want to use and click **Save**.

DRA Server Connection

The configuration for the DRA Service connection includes setting a default server location, modifying the port (if needed), and a connection timeout, in seconds. You can also disable the setting with the toggle switch.

When providing the DRA Server location, use the format shown in the example below:

```
ServerName.DomainName.com
```

Customizing the Web Console

You can customize object properties in the Web Console. When implemented correctly,

property customizations will help to automate tasks with object management.

Customizing Property Pages

If you have DRA Administration powers, you can customize the object property forms that you use in your Active Directory management role by object type. This includes creating and customizing new object pages that are based on object types that are built into DRA. You can also modify properties for the built-in object types.

Property objects are clearly defined in the Property Pages list in the Web Console so you can easily identify which object pages are built-in, which built-in pages are customized, and which pages are not built-in and were created by an administrator.

Customizing an Object Property Page

You can customize object property forms by adding or removing pages, modifying existing pages and fields, and by creating custom handlers for property attributes. The custom handlers on a field are executed whenever that field's value is modified. The timing can be configured as well, so the administrator can specify if the handlers should be run immediately (on every key press), when the field loses focus, or after a specified time delay.

The object list in Property Pages provides operation types for each object type, Create Object and Edit Properties. These are the principal operations your assistant administrators perform in the Web Console. They perform these operations by navigating to **Management** > **Search** or **Advanced Search**. Here they can create objects from the Create pull-down menu or edit existing objects selected in the search results table through the Properties icon

To customize an object property page in the Web Console:

1. Log in to the Web Console with DRA Administration privileges.

2. Navigate to **Administration** > **Customization** > **Property Pages**.

3. Select an object and operation type (Create Object or Edit Object) in the Property Pages list.

4. Click the **Properties** icon ✐ .

5. Customize the object property form by doing one or more of the following, and then apply your changes:

   ○ Add a new property page: **+ Add Page**

   ○ Reorder and delete property pages

   ○ Select a property page and customize the page:

      ▪ Reorder configuration fields on the page: ↑ ↓

      ▪ Edit fields or subfields: ✐

      ▪ Add one or more fields: ＋ or **Insert a new Field**

      ▪ Remove one or more fields: 🗑

   ○ Create custom handlers for properties by using scripts, message boxes, or queries (LDAP, DRA, or REST)

      For more information about using custom handlers, see "Adding Custom Handlers", in the DRA Administrator Guide.

Creating a New Object Property Page

To create a new object property page:

1. Log in to the Web Console with DRA Administration powers, and navigate to **Administration** > **Customization** > **Property Pages**, and click ➕ **Create**.

2. Create the initial object properties form by defining its name, icon, object type, and operation configuration.

   After clicking OK, Create actions are added to the Create drop-down menu while Property actions display in object form when the user selects and edits an object from the search list.

3. Customize the new form as required. See Customizing an Object Property Page.

Managing Objects in the Web Console

You manage objects in the Web Console by navigating to the Management masthead. From here, you can search by object type for objects in managed domains, Entra ID tenants, containers, and the Recycle Bin. Within a domain or Entra ID tenant, you can manage and take actions on Active Directory and Entra ID Active Directory objects using DRA.

If you select an object in the search results list, all applicable actions that you can take on that object are available on the taskbar above the grid. The options available are based on the object type selected, the components currently configured for DRA, and your assigned administrator privileges.

To edit an object's properties, mouse over the object and click the **Properties** icon ✎ that appears on the object row. From here, you can access all the object's Properties pages in the left navigation pane.

> **Important**
>
> If you want to **protect an object from accidental deletion**, scroll to the bottom of the **General** Properties page, select the check box to enable this feature, and **Apply** the changes.

For more information about actions you can take on objects, see the following topics:

- Managing Active Directory Objects

- Managing Exchange Mailboxes and Public Folders

- Managing Resources

Generating Change History Reports

opentext™

If Change History is configured by your DRA Administrator and you have the **Generate UI Reports** power, you can generate change history reports, and export reports for managed objects in DRA. This includes changes made in DRA and outside of DRA. You can only generate change history reports from the Web Console, which includes the following types of reports:

- Changes made by the user

- Changes made to the user

- User mailboxes created by the user

- User mailboxes deleted by the user

- Group and contact email addresses established by the user

- Group and contact email addresses deleted by the user

- Virtual attributes created or disabled by the user

- Objects moved by the user

To generate Unified Change History (UCH) reports:

1. Launch the Web Console.

2. Go to **Management > Search**.

3. Define the search criteria using the **Search by**, **search term**, **OBJECTS**, and **SCOPE** options.

4. Click the **Search** button to display the search results.

5. Select the objects for which you want to generate reports.

6. Click the **View Change History Reports** icon 🗓 .

   In the Unified Change History Report form, you can edit and generate your report criteria from the **Type**, **Target object(s)**, **Date Range, and Maximum Rows** options, to include defining the servers where the changes are detected (DRA and Change Guardian).

7. Click **Generate** to fetch audit data and to generate a UCH report.

8. You can sort and export the report into a required format such as CSV and HTML.

To create a CSV file of the displayed report, you can export all of the changes generated or just those displayed on the current page, by executing one of the following options after generating the report using the steps above:

- Click **Export All** ⤓ and save the exported report.

- Click **Export Current Page** ⤵ and save the exported report.

If needed, you change the number of changes that show on the page, up to 200 items.

Using Workflow Automation

Using Workflow Automation you can automate IT processes by launching workflow forms that run on the execution of a workflow or when triggered by a named workflow event that is created in the Workflow Automation server.

Workflow forms, when created or modified, are saved to the Web Server. When you log on to the Web Console for this server, you will have access to the forms based on delegated powers and how the forms are configured. Forms are generally available to all users with web server credentials. The capability to submit the form requires appropriate powers.

Launching a workflow form: Workflows are created in the Workflow Automation Server, which must be integrated with DRA via the Web Console. To save a new form, you must have either the **Launch Specific Workflow** or **Trigger Workflow by Event** option configured in the form properties. More information about these options is provided below:

- **Launch Specific Workflow:** This option lists all the available workflows that are in production in the Workflow Server for DRA. For the workflows to populate in this list, they need to be created in the `DRA_Workflows` folder in the Workflow Automation server.

- **Trigger Workflow by Event:** This option is used to execute workflows with pre-defined triggers. The workflows with triggers are also created in the Workflow Automation server.

> **Note**
>
> Only workflow forms configured with Launch Specific Workflow will have an execution history that can be queried in the main search pane under **Tasks** > **Requests**.

More information about Workflow Automation is included in the following guides on the DRA documentation site:

- DRA Administrator Guide

- WFA Administrator Guide

- WFA User Guide

- WFA Process Authoring Guide

1.2.2. Account and Resource Management

The Account and Resource Management node in the Delegation and Configuration Console provides access to most of the DRA assistant administrator tasks, addressing enterprise management needs from basic administration to advanced Help Desk issues. Using Account and Resource Management, you can perform account and resource management tasks and manage Microsoft Exchange mailboxes.

Account and Resource Management contains the following nodes:

All My Managed Objects

Enables you to manage objects, such as user accounts, groups, contacts, resources, dynamic groups, dynamic distribution groups, resource mailboxes, and public folders for each domain in which you have some power.

Temporary Group Assignments

Enables you to manage group memberships for users who only need group membership for a specific period.

Advanced Queries

Enables you to manage advanced queries available on the Administration server.

Recycle Bin

Enables you to manage deleted user accounts, groups, contacts, and resources, for any Microsoft Windows domain where the Recycle Bin is enabled.

To access the Account and Resource Management node, click **Delegation and Configuration** in the NetIQ Administrator program folder and expand the Delegation and Configuration node in the console.

When you start the Delegation and Configuration console, you initially connect to the best available Administration server in the local domain. The best-available Administration server is the closest server, which is typically a server in the network site. By seeking the best available Administration server, DRA provides a quicker connection and improved performance.

To learn more about working in Account and Resource Management, see the following topics:

- Connecting to an Administration Server or Managed Domain

- Modifying the Console Title

- Customizing List Columns

- Managing Objects in Account and Resource Management

- Executing Saved Advanced Queries

- Restoring Console Settings

- Special Characters Restrictions

- Using Wildcard Characters

- Viewing Your Assigned Powers and Roles

- Viewing the Product Version Number and Installed Hotfixes

- Viewing Your Current License

- Recovering a BitLocker Password

Connecting to an Administration Server or Managed Domain

By default, DRA connects to the best available Administration server for a managed domain or computer. The best available Administration server is the closest server, which is typically a server in the network site. If the site does not include an Administration server, DRA connects to the next available server in the managed domain or managed subtree. You can also specify the Administration server or domain to which you want to connect.

When you first start the user interfaces, DRA initially connects to the domain of your logon account. If you are logged on to a domain that is not managed by an Administration server, or if DRA cannot connect to the Administration server for that domain, DRA may display an error message. Ensure the Administration server is available and try again.

To connect to an Administration server:

1. On the File menu, click **Connect to DRA server**.

2. Click **Connect to this DRA server**.

3. Type the name of the Administration server, using the following format: *computername*.

4. Click **OK**.

To connect to a managed domain or computer:

1. On the File menu, click **Connect to DRA server**.

2. Select the appropriate option, and then type the name of the managed domain or computer.

3. For example, to connect to the HOULAB domain, click **Connect to a DRA server that manages this domain**, and then type `HOULAB`.

4. To specify an Administration server for the managed domain or computer, click **Advanced**, and then select the appropriate option.

5. Click **OK**.

Modifying the Console Title

You can modify the information displayed in the title bar of the Delegation and Configuration console. For convenience and clarity, you can add the user name with which the console was launched and the Administration server to which the console is connected. In complex environments in which you need to connect to multiple Administration servers using different credentials, this feature helps you quickly discern which console you need to use.

To modify the console title bar:

1. Start the Delegation and Configuration console.

2. Click **View** > **Options**.

3. Select the Window Title tab.

4. Specify the appropriate options, and then click **OK**.

Customizing List Columns

You can select which object properties DRA displays in list columns. This flexible feature enables you to customize the user interface, such as lists for search results, to better meet the specific demands of administrating your enterprise. For example, you can set columns to display the user logon name or group type, letting you quickly and effectively find and sort the data you need.

To customize list columns:

1. Select the appropriate node. For example, to choose which columns display when viewing search results on managed objects, select **All My Managed Objects**.

2. On the View menu, click **Choose Columns**.

3. From the list of properties available for this node, select the object properties you want to show.

4. To change the column order, select a column, and then click **Move Up** or **Move Down**.

5. To specify the column width, select a column, and then type the appropriate number of pixels in the provided field.

6. Click **OK**.

Managing Objects in Account and Resource Management

You manage objects in Account and Resource Management by selecting **All My Managed Objects** or a sub-node in the directory tree. From here, you can search by object type for objects in domains, containers, and OUs.

If you select an object in the search results list, all applicable actions that you can take on that object are available in the **Tasks** menu on the toolbar or in right-click menu. The options available are based on the object type selected, the components currently configured for DRA, and your assigned administrator privileges.

To edit an object's properties, select the object and click **Properties** in the **Tasks** menu. From here, you can access all the object's Properties pages by clicking page links in the left navigation pane.

> **Important**
>
> If you want to **protect an object from accidental deletion**, select the object and open **Properties**, select **General** in the navigation pane, select the check box to enable this feature, and **Apply** the changes.

For more information about actions you can take on objects, see the following topics:

- Managing Active Directory Objects

- Managing Exchange Mailboxes and Public Folders

- Managing Resources

Executing Saved Advanced Queries

Using advanced queries, you can search for users, contacts, groups, computers, printers, OUs, and any other object that DRA supports. If you have the Execute Saved Advanced Queries power, you can execute advanced queries available in the **Saved Queries** list for any container in the Account and Resource Management node. For more information about your assigned powers, see Viewing Your Assigned Powers and Roles.

To execute saved advanced queries:

1. Expand **Account and Resource Management** > **All My Managed Objects**.

2. Select the appropriate container. For example, if you want DRA to search for user account information, select **Users**.

3. To view the advanced search pane, click **Advanced Search**.

4. In the advanced search pane, select an Advanced Search query from the **Saved Queries** list.

5. Click **Load Query**, and then click **Find Now**.

Restoring Console Settings

DRA enables you to resize windows and then persists your window sizes. DRA also persists many other settings, including the last Administration server to which you connect, the columns you add or remove from list results, and column widths. If you want to restore these settings to the original setting with which you installed DRA, the Restore Default Settings option enables you to do so.

To restore default console settings:

1. Click **View** > **Options**.

2. Select the **Saved Settings** tab.

3. Review the information provided on the window, and then click **Restore Default Settings**.

Special Characters Restrictions

You cannot use the following special characters when naming user accounts, groups, contacts, OUs, computers, ActiveViews, AA groups, roles, policies, or automation triggers. These naming restrictions apply to the name of the object as well as the name of the rule that defines the object.

Naming user accounts, groups, and computers

When specifying a pre-Windows 2000 name, you cannot use the following special characters:

Backslash	\
Colon	:
Comma	,
Double quote	"
Equal sign	=
Forward slash	/
Greater than	>
Left bracket	[
Less than	<
Plus sign	+
Right bracket	]
Semi colon	;
Vertical bar	|

Important

For Public Folder Management the Backslash \ character is not supported.

When naming user accounts, groups, and computers in Microsoft Windows domains, you can use any special character.

Naming contacts and OUs

When naming contacts and OUs, you can use any special character.

Naming ActiveViews, AA groups, and roles

When naming ActiveViews, AA groups, and roles, you cannot use the backslash (\).

Naming policies and automation triggers

When naming policies and automation triggers, you cannot use the backslash (\).

Invalid Characters in Entra ID

Invalid characters will cause the synchronization between Entra ID Active Directory and your on-premises directory to fail. See the Directory object and attribute preparation

subtopic on the Microsoft Office support website to learn more about these invalid characters.

To ensure that these characters are not used in your online mailbox properties, do the following:

1. Click the Configuration Management node in the Delegation and Configuration console, and select **Update Administration Server Options**.

2. Click **Entra ID Sync** in the tab menu.

3. Click **Enforce online mailbox policies for invalid characters and character length**, and click **OK**.

Using Wildcard Characters

DRA supports wildcard characters in many fields in the DRA consoles and in CLI commands. Wildcards enable you to define rules that match multiple objects to a specific condition or standard, such as a naming convention. You can use wildcards instead of regular expressions to narrow or broaden the scope of the rule. Wildcard matching is not case-sensitive. You can also use the question mark (?), asterisk (*), or number sign (#) wildcard characters as normal characters by prefixing a backslash (\) to the particular wildcard character. For example, to search for abc*, type the search text abc*.

DRA supports the following wildcard characters. You cannot use wildcard characters in names.

Match Item	Character	Definition
Any character	Question mark ?	Matches exactly one character
Any digit	Number sign #	Matches one digit
Any character, 0 or more matches	Asterisk *	Matches zero or more characters

The following table provides examples of wildcard character specifications and what they match and do not match.

Example	Matches	Does Not Match
Den???	Denton and Dennis	Denison
El ????o	El Campo and El Indio	El Paso
Houston, TX #####	Houston, TX 77024	Houston, TX USOFA

DRA does not support wildcard specifications that contain logical operations.

Viewing Your Assigned Powers and Roles

Roles and powers define how you manage objects. A role is a set of powers that provides the permissions required to perform a specific administration task, such as creating a user account or moving shared directories.

The DRA Administrator assigns roles, adds you to specific AA groups, and associates you with ActiveViews (sets of domain objects you can manage). You can view these assignments through the Delegation and Configuration console. You do not need any auxiliary powers to view the roles and powers assigned to you.

To view your assigned powers and roles:

1. On the File menu, click **DRA Properties**.

2. Click **Powers**.

3. Select the appropriate view. For example, click **Flat View** to see a table of your AA group memberships, assigned powers and roles, and associated ActiveViews.

4. Expand the appropriate item. For example, under **Has Power** column, expand **Roles and Powers** to view the individual roles or powers assigned to you.

5. Click **OK**.

Viewing the Product Version Number and Installed Hotfixes

You can view the product version number and installed hotfixes from the DRA Properties window. This window provides version numbers and lists of installed hotfixes for the Administration server and the DRA client computer.

To view the product version number and installed hotfixes:

1. On the File menu, click **DRA Properties**.

2. Click **General**.

3. View the information you need.

4. Click **OK**.

Viewing Your Current License

DRA requires a license key file. You can view your product license from any Administration server computer. You do not need any auxiliary powers to view the product license.

To view your license:

1. On the File menu, click **DRA Properties**.

2. Click **License**.

3. Review the license properties, and then click **OK**.

Recovering a BitLocker Password

Microsoft BitLocker stores its recovery passwords in Active Directory. With the required powers, you can use the DRA BitLocker Recovery feature to find and recover lost BitLocker passwords for end users.

> **Important**
>
> Before using the BitLocker Recovery Password feature, ensure that your computer is assigned to a domain and BitLocker is turned-on.

Viewing and Copying a BitLocker Recovery Password

If the BitLocker password for a computer is lost, it can be reset using the Recovery Password key from the computer's properties in Active Directory. Copy the password key and provide it to the user.

To view and copy the recovery password:

1. Launch the Delegation and Configuration console and navigate to **Account and Resource Management** > **All My Managed Objects**.

2. Select the domain, and execute a search to list all computers in the domain.

3. In the computers list, right-click the required computer, and select **Properties** > **BitLocker Recovery Password**.

4. Right-click and copy the BitLocker recovery password, and paste the password text into a text file.

Finding a Recovery Password

If the name of a computer was changed, the Recovery Password must be searched for in the domain using the first eight characters of the Password ID.

> **Note**
>
> To search for the Recovery Password, the assistant administrator must have the **View BitLocker recovery password** power on the domain containing the delegated computer objects.

To find a recovery password by using a password ID:

1. Launch the Delegation and Configuration console and navigate to **Account and Resource Management** > **All My Managed Objects**.

2. Right-click the **Managed Domain**, and then click **Find BitLocker Recovery Password**.

   To find the first eight characters of the recovery password, see Viewing and Copying a BitLocker Recovery Password.
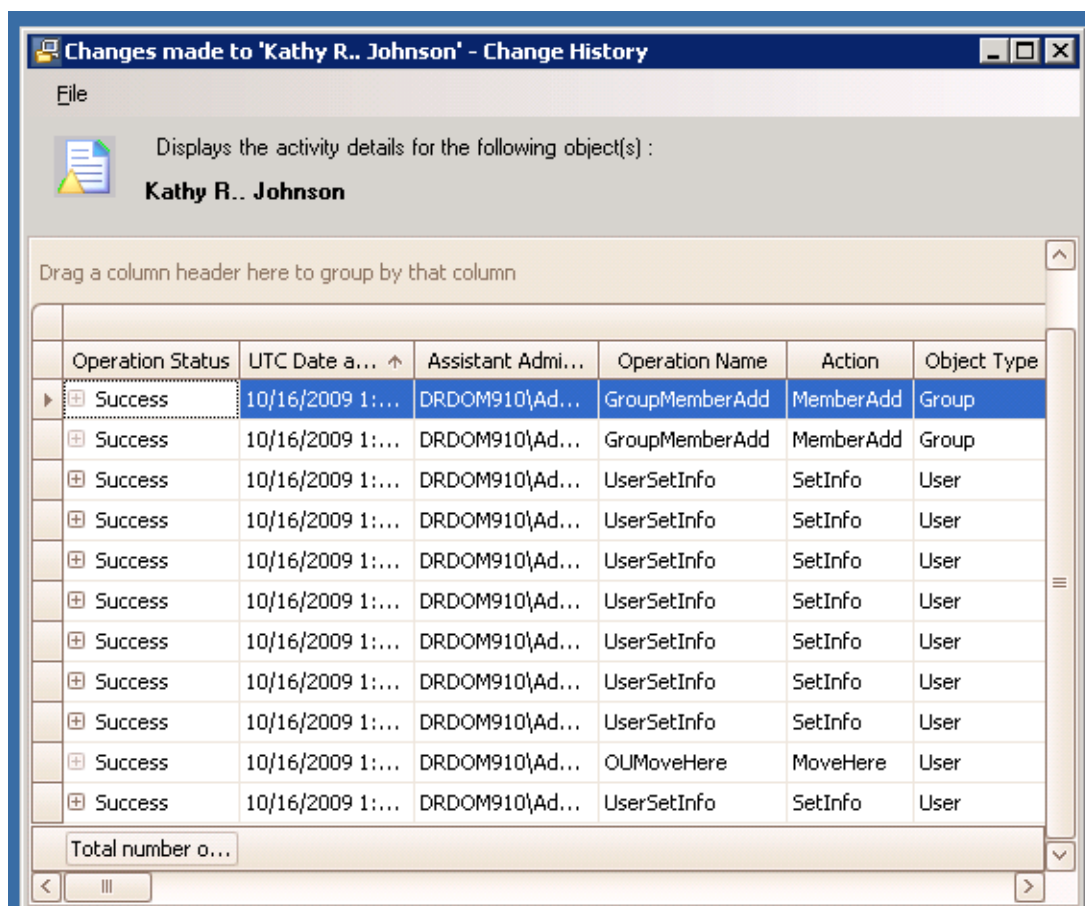
3. In the **Find BitLocker Recovery Password** page, paste the copied characters in the search field, and then click **Search**.

1.2.3. DRA reporting

DRA Reporting provides built-in, ready-to-use reports that let you quickly track duplicate accounts, last account logons, Microsoft Exchange mailbox details, and much more. Reporting also provides real-time details of changes made in your environment, including before and after values for changed properties. You can export, print, or view reports, or publish them to SQL Server Reporting Services.

DRA provides two methods of generating reports that enable you to collect and review user account, group, and resource definitions in your domain: **Activity Detail reports** and **DRA Management reports**. Activity Detail reports, viewed through the Delegation and Configuration console, provide real-time change information for objects in your domain. For example, you can view a list of changes made to an object or by an object during a specified time period using Activity Detail reports.

The following figure shows a sample Activity Detail report:

Optional **DRA Management reports**, viewed through the NetIQ Reporting Center (Reporting Center), provide activity, configuration, and summarization information about events in your managed domains. Some Management reports are available as graphical representations of the data. These built-in reports can also be customized to give you exactly the information you need.

For example, you can view a graph showing the number of events in each managed domain during a specified time period using Management reports. Reporting enables you to view

details about the DRA security model, such as ActiveView and AA group definitions.

You must install and configure the optional Management reports before you can view these reports. For more information about installing reporting components, see the *Installation Guide*. For more information about DRA Reporting, see DRA Reporting.

Start the Reporting Center Console in the NetIQ > Reporting Center program group.

The following figure shows the Reporting Center interface with DRA Management reports selected.
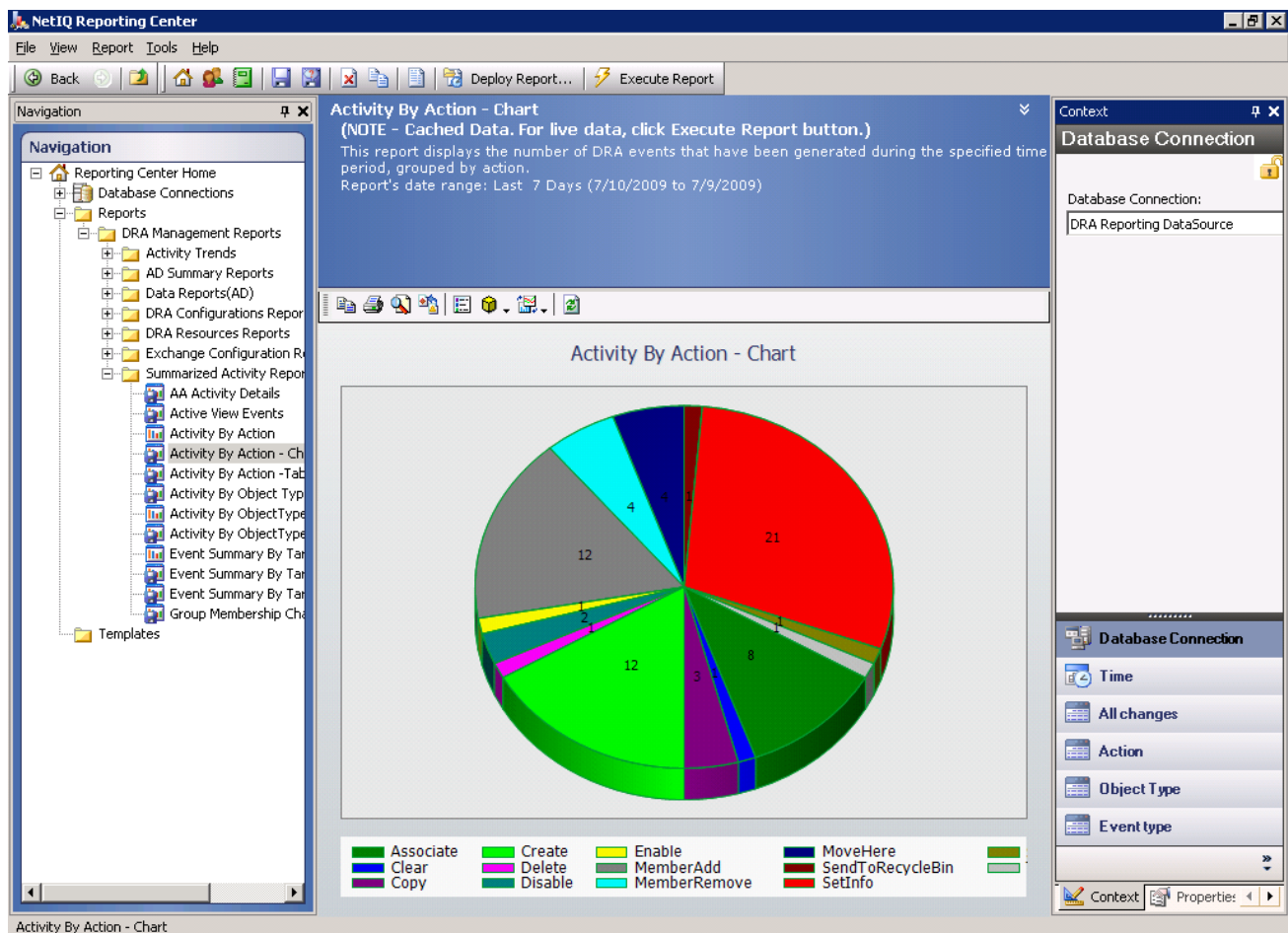
To learn more about DRA Reporting, see the following topics:

- Understanding DRA Reporting

- How DRA Uses Log Archives

- Understanding Dates and Times

- DRA Reporting Tasks

Understanding DRA Reporting

DRA Reporting provides two methods of generating reports that enable you to see the latest changes in your environment and to collect and review user account, group, and resource definitions in your domain.

Activity Detail reports

Accessed through the Account and Resource Management node of the Delegation and Configuration console, these reports provide real-time change information for objects in your domain.

DRA Management reports

Accessed through NetIQ Reporting Center (Reporting Center), these reports provide activity, configuration, and summarization information about events in your managed domains. Some reports are available as graphical representations of the data.

For example, you can view a list of changes made to an object or by an object during a specified time period using Activity Detail reports. You can also view a graph showing the number of events in each managed domain during a specified time period using Management reports. Reporting also enables you to view details about the DRA security model, such as ActiveView and AA group definitions.

DRA disables functions and reports that your license does not support. You must also have the appropriate powers to run and view reports. Therefore, you may not have access to some reports.

DRA Management reports can be installed and configured as an optional feature and are viewed in Reporting Center. When you enable and configure data collection, DRA collects information about audited events and exports it to a SQL Server database on a schedule that you define. When you connect to this database in Reporting Center, you have access to over 60 built-in reports:

- Activity reports that show who did what, and when

- Configuration reports that show the state of AD or DRA at a specific point in time

- Summarization reports that show activity volume

For more information about configuring data collection for Management reports, see the *Administrator Guide*.

How DRA Uses Log Archives

To review and report on assistant administrator actions, DRA logs all user operations in the log archive on the Administration server computer. User operations include all attempts to change definitions, such as updating user accounts, deleting groups, or redefining ActiveViews. DRA also logs specific internal operations, such as Administration server initialization and related server information. In addition to logging these audit events, DRA logs the before and after values for the event so that you can see exactly what changed.

DRA uses a folder, **NetIQLogArchiveData**, called a **log archive** to securely store archived log data. DRA archives the logs over time and then deletes older data to make room for newer data through a process called grooming.

DRA uses the audit events stored in the log archive files to display Activity Detail reports, such as showing what changes have been made to an object during a specified time period. You can also configure DRA to export information from these log archive files to a SQL Server database that NetIQ Reporting Center uses to display Management reports.

DRA always writes audit events to the log archive. You can enable or disable having DRA write events to the Windows event logs as well.

For more information about DRA auditing, see the _Administrator Guide_.

Understanding Dates and Times

DRA uses the **Short date style** and **Time style** specified in the Regional Settings application in Control Panel for report display. DRA reports show UTC date and time as well as local date and time for events. DRA reports support the following date formats:

- `m/d/yy`
- `m-d-yy`
- `m/d/yyyy`
- `m-d-yyyy`
- `mm/dd/yy`
- `mm-dd-yy`
- `mm/dd/yyyy`
- `mm-dd-yyyy`
- `dd/mm/yy`
- `dd-mm-yy`
- `dd/mm/yyyy`
- `dd-mm-yyyy`

DRA Reporting Tasks

To generate DRA Management reports, install Reporting Center and enable data collection in DRA. For more information about enabling data collection, see the *Administrator Guide*. To generate Activity Detail reports, right-click over any object and click **Reporting** to see your choices for reports on that object. The following sections guide you through the various Reporting tasks.

Viewing Activity Detail Reports

Activity Detail reports display information about changes in your environment. You can view or print a report, as well as save a report in Excel, CSV, or TXT format. To view or print reports, you must be associated with the Reporting Administration role.

When viewing reports, enter criteria to specify the time period you want to display information about. You can also choose to view a report limited to changes made on specific DRA servers, and you can limit the number of rows to be included in the report. If the report size exceeds one of the following limits, DRA displays a message stating that the report is not complete:

- Size exceeds 500 MB

- Time needed to query all DRA servers exceeds 5 minutes

- Number of rows to be displayed exceeds 1000

You have the option of viewing the report containing only the information retrieved before reaching one of these limits, or you can change the report criteria to view a report that meets these limits.

To view a report:

1. In the left pane, expand **All My Managed Objects**.

2. To specify the object for which you want to view a report, complete the following steps:

   1. *If you know the object location*, select the domain and OU that contains this object.

   2. In the search pane, specify the object attributes, and then click **Find Now**.

3. In the list pane, right-click the object and click **Reporting**.

4. Select the type of report, such as **Changes made to objectName** or **Changes made by objectName**. The available reports vary depending on the type of object you have selected.

5. Select the start and end dates to specify the changes you want to view.

6. *If you want to change the number of rows to be displayed*, type a number over the default value of 250.

   > **Note**
   >
   > The number of rows displayed applies to each Administration server in your environment. If you include 3 Administration servers in the report and use the default value of 250 rows to display, up to 750 rows can be displayed in the report.

7. *If you want to include only specific Administration servers in the report*, select **Restrict query to these DRA servers** and type the server name or names you want the report to include. Separate multiple server names with commas.

8. Click **OK**.

   > **Note**
   >
   > DRA might take up to 5 seconds to display recent changes in reports. Therefore, wait at least 5 seconds after making a change before you attempt to view a report that contains the change.

Exporting Activity Detail Reports

You can export Activity Detail reports in the following formats: XLS, CSV, and TXT. The default format is Microsoft Excel format.

To export Activity Detail reports:

1. In the report window, on the File menu, click **Preview and Export**.

2. In the Preview window, on the File menu, click **Export Document** > **Excel File**.

3. Select your export options and click **OK**.

4. In the Save as window, type a name for the file and click **Save**.

Printing Activity Detail Reports

To print reports, you must be associated with the Reporting Administration role. You can view or print Activity Detail reports, as well as save a report in various formats.

To print Activity Detail reports:

1. In the report window, on the File menu, click **Preview and Export**.

2. In the Preview window, on the File menu, click **Print**.

Viewing Management Reports

You must install DRA Reporting and configure the DRA data collectors to be able to view Management reports in Reporting Center. For more information about installing DRA Reporting and configuring the DRA Collectors, see the *Administrator Guide*.

When you log on to the Reporting Center, the Web Service uses IIS to validate the account credentials according to the way you configured the Web Service during installation.

To view Management reports:

1. Log on to the computer that is running the Reporting Center Console.

2. Start **Reporting Center Console** in the NetIQ > Reporting Center program group.

3. Provide the required information in the Logon dialog box and click **Logon**.

4. In the Navigation pane, expand **Reports** > **DRA Management Reports**.

5. Expand the report categories until you find a report you want to view.

6. Click the report name in the Navigation pane and the report will load in the center Results pane, displaying cached data.

7. *If you want to see the report using the latest data,* click **Execute Report** in the Results Pane.

You can change the default context settings to display different report results. For more information about context settings in Reporting Center, see the *Administrator Guide*.

Customizing Management Reports

More than 60 Management reports are shipped with DRA. Reporting Center gives you the flexibility to customize and deploy these reports in many ways. For more information about customizing and deploying Management reports in Reporting Center, see the *Administrator Guide*.

To customize a Management report:

1. View a report that is similar to a report you want to create. For more information, see Viewing Management Reports.

2. Customize the report by changing the report properties and context settings to display the information you want.

3. Click **Execute Report**.

4. On the Report menu, click **Save Report As** and specify a report title and location to save the new report.

5. Click **Save**.

For more information about working with Management reports in Reporting Center, see the *Administrator Guide*.

1.3. Managing Active Directory Objects

This chapter contains conceptual and procedural information for managing user accounts, groups, dynamic groups, dynamic distribution groups, and contacts in both the Account and Resource Management node of the Delegation and Configuration console and in the Web Console. The information for User accounts is more comprehensive to provide an example of how you manage objects in general in both client applications.

- Managing User Accounts

- Managing Groups

- Managing Dynamic Distribution Groups

- Managing Dynamic Groups

- Managing Contacts

- Managing Group Managed Service Accounts

1.3.1. Managing User Accounts

Microsoft Windows relies on the user account type to determine access permissions for the associated user account. A user account can be global or local. DRA also supports InetOrgPerson objects, but recognizes InetOrgPerson objects as normal users.

Global user account

A user account that can be used in any domain that trusts the domain in which the user account was created. You can grant specific permissions to a user account. You can also make a user account a member of a group and then assign permissions to that group. Grouping user accounts helps simplify the process of managing network permissions for many user accounts.

Local user account

A local user account is the same as any account that you use to log into a Windows operating system. It enables you to access the system's resources in your own user space.

To learn more about managing user accounts, see the following topics:

- User Accounts in Trusted Domains

- User Account Management Tasks

- Transforming User Accounts

User Accounts in Trusted Domains

Microsoft Windows stores user account and group definitions in the directory of the managed domain. Therefore, an Administration server cannot modify the directory information from a trusted domain unless that domain is also managed by DRA.

For example, in Account and Resource Management, you may see user accounts and groups that you cannot modify. These user accounts and groups are defined in domains trusted by one of the managed domains. However, you can add accounts and groups from a trusted domain to other groups in the managed domain.

User Account Management Tasks

This section guides you through administering user accounts in the Account and Resource Management node of the Delegation and Configuration Console and in the Web Console. With the appropriate powers, you can perform various user account management tasks, such as creating and deleting accounts. If you select multiple user accounts, you can perform selected tasks in one operation, such as deleting, moving, or adding users to a group. For more information about your assigned powers, see Viewing Your Assigned Powers and Roles.

User Account Tasks in Account and Resource Management

You can execute all applicable tasks below from the **Tasks** menu or from the right-click menu. Generally, you select the **All My Managed Objects** node and execute a **Find Now** operation to locate and select the desired user object. In the case of creating a new user, you must select the domain or OU where you want to create the user. The Tasks menu indicates which tasks you can perform when you select single or multiple user accounts.

Manage your own account

You can manage your own account by modifying general properties, such as your telephone number. Before you manage your account, ensure you have the appropriate power.

Copy a user account to another ActiveView

You can copy a user account to another ActiveView. This action is called transferring a user account. To copy a user account to another ActiveView, you need the Copy User to Another ActiveView power in both the source and target ActiveViews. Transferring a user account to another ActiveView does not remove the user account from the source ActiveView.

> **Note**
>
> Copying a user account to another ActiveView can only be done from the Delegation and Configuration Console via the Account and Resource Management node.

Rename a user account

You can rename user accounts in the managed domain or managed subtree. Changing the user logon name also changes the name of the mailbox associated with the user account.

User Account Tasks in the Web Console

You can execute most of the tasks below from the **Management** > **Search** tab in the Web Console. Execute a search operation to locate and select the required user object. After you select one or more objects in the list, the taskbar becomes active with toolbar options and drop-down options for **Accounts** and **Exchange**. Mouse over a toolbar icon or click on a drop-down menu to display their functions or options.

Create a user account

You can create user accounts in the managed domain or managed subtree. You can also modify properties, create a mailbox, enable email, and specify group memberships for the new account.

> **Note**
>
> - Your company may have a naming convention enforced through policy that determines the name you can assign to the new user account.
>
> - By default, DRA places the new user account in the Users OU of the managed domain.
>
> - You cannot create InetOrgPerson objects in DRA.

Clone a user account

When you clone a user account, any groups that the user is a member are automatically added to the new user account, saving you time in configuring the new account. You can add or remove groups from the new account, enable email, and make any other property configurations as you would with any new account.

> **Note**
>
> When you clone an InetOrgPerson object, you create a user account.

Modify user account properties

You can manage the properties of user accounts in the managed domain or managed subtree. The powers you have determine which properties you can modify for a user account. If you installed Exchange and enabled Microsoft Exchange support, you can modify the associated mailbox properties while managing user accounts.

> **Note**
>
> If home directory policies are enabled, DRA automatically modifies the home directory of a user account when you manage that account. For example, when you change the home directory location, DRA attempts to create the specified home directory and move the contents of the previous home directory to the new location. DRA also applies the assigned ACLs from the previous directory to the new directory.

> **Note**
>
> DRA enables you to export the **Member Of** results as a CSV file. To export the **Member Of** results from the Web Console, go to **Management** > **Search** and click **Properties**. Navigate to the **Member Of** tab and click the **Download** icon. The unsaved changes are not exported. Ensure you save any recent changes so they are available in the exported file.

Enable a user account

You can enable a user account in the managed domain or managed subtree. If you are managing a Microsoft Windows account, you can specify the domain controller at which DRA applies this change.

When you apply this change to a specific domain controller, DRA also applies this change to the default domain controller for this managed domain. To verify which default domain controller DRA is using, view the domain properties.

Disable a user account

You can disable a user account in the managed domain. If you are managing a Microsoft Windows account, you can specify the domain controller at which DRA applies this change.

When you apply this change to a specific domain controller, DRA also applies this change to the default domain controller for this managed domain. To verify which default domain controller DRA is using, view the domain properties.

Unlock a user account

You can unlock a user account in the managed domain or managed subtree.

Because DRA retrieves the user account status from the accounts cache, the user interface may indicate that the selected account is unlocked when it is locked. DRA allows you to unlock a user account even if the account status indicates it is currently unlocked. You can also specify a domain controller when unlocking a user account using the DRA console without having to reset the user account password.

Reset a user account password

You can reset the password for an account in the managed domain or managed subtree. The powers you have determine the fields you can change for that user account.

When you reset the password for a user account, DRA automatically unlocks the account. You can select whether DRA generates a new password for the user account. You can also modify several password-related options for the account. If you are managing a Microsoft Windows account, you can specify the domain controller at which DRA applies these changes

> **Note**
>
> When you apply this change to a specific domain controller, DRA also applies this change to the default domain controller for this managed domain. To verify which default domain controller DRA is using, view the domain properties.

Move a user account to another container

You can move a user account to another container, such as an OU, in the managed domain or managed subtree.

Delete a user account

You can delete a user account in the managed domain or managed subtree. If the

Recycle Bin is disabled for that domain, deleting a user account permanently removes the user account from Active Directory. If the Recycle Bin is enabled for that domain, deleting a user account moves the user account to the Recycle Bin.

> **Caution**
>
> When you create a user account, Microsoft Windows assigns a Security Identifier (SID) to that account. The SID is not generated from the account name. Microsoft Windows uses SIDs to record privileges in access control lists (ACLs) for each resource. If you delete a user account, you cannot return access capabilities for that account by creating a new user account with the same name.

Specify group membership for user accounts

You can add or remove user accounts from a specific group in the managed domain or managed subtree. You can also view or modify properties of existing groups to which this account belongs.

Transforming User Accounts

DRA offers you the ability to quickly and efficiently transform user accounts. When the individual associated with a user account transitions to new job responsibilities, you can use the transform capabilities of DRA. Taking advantage of job role templates, you can quickly add, remove, or update the group memberships associated with an account. Whether an individual is promoted, changes departments, or leaves the company, the ability to transform a user account will save you time, money, and guesswork.

Understanding the Transformation Process

You can use the transform user account capabilities to fulfill any of the following needs:

- Remove group memberships from a user account

- Add group memberships to a user account

- Change user properties

- Remove particular group memberships while adding other group memberships to a user account

Consider the following process before attempting to transform a user account:

1. Decide whether you need to add, remove, or both add and remove group memberships.

2. Review your current subtractive and additive templates to ensure you have the necessary template user accounts.

3. If necessary, create any required template accounts.

4. Complete the Transform User wizard.

As DRA transforms a user, the group memberships designated by the subtractive template are removed from the user account, while those memberships designated by the additive template are assigned to the user account. DRA leaves any memberships outside of the subtractive or additive templates intact. For example, an individual in your outside sales department is transferred from US sales to European sales. Within your organization, you have both distribution groups and security groups that are unique for these sales teams and a number that is shared across all sales teams. The US sales team has the US Hotspots DL and the US Sales Mgmt DL distribution groups while the European sales team has Euro Hotspots and Euro Sales Mgmt distribution groups. Both teams are members of the Global Sales Sec security group, but also have individual site-specific security groups.

Your subtractive template, named US Sales Template, would be assigned the following group memberships:

- US Hotspots DL

- US Sales Mgmt DL

- Global Sales Sec

- US Sec

Your additive template, named Euro Sales Template, would be assigned the following group memberships:

- Euro Hotspots DL

- Euro Sales Mgmt DL

- Global Sales Sec

- Euro Sec

During the transformation process, the user account of the transferred sales person is first removed from all the group memberships designated by the US Sales Template, and then added to all the group memberships designated by the Euro Sales Template. If this individual was also a member of the Poker Players distribution group, this group membership remains untouched.

The following powers allow an assistant administrator to further modify a user account during the transformation process:

- Modify Address Properties while Transforming a User Account

- Modify Description while Transforming a User Account

- Modify Office while Transforming a User Account

- Modify Telephone Properties while Transforming a User Account

You can also restrict the ability to add or remove group memberships by giving an assistant administrator only one of the following powers:

- Add a user to groups found in a template

- Remove a user from groups found in a template

You can use either of these power-based limiting options to create a layer of security within your organization. By giving certain individuals the power to only remove groups found in a template, you can create interim user accounts. These interim accounts can then be reviewed before a different assistant administrator uses an additive template account to grant the new group memberships.

Creating User Transformation Templates

Transformation of user accounts is directly tied to the roles and job ladders of your organization. Consider creating a template for each role or job within your company. DRA makes no distinction between a user account template used as subtractive versus additive. Create a single template user account for each role within your organization. During the transformation, you select the template as subtractive or additive. Selecting a template as subtractive does not stop the same template from being used as additive in a future transformation.

To create a user transformation template, you must have the powers to create a user account and assign that user account to the appropriate groups. These powers can be obtained through associating your account with the Create and Delete User Accounts and the Group Administration roles in the appropriate ActiveViews or through the assigning of individual powers.

Transforming User Accounts

Transforming a user account enables you to add, remove, or both add and remove user account group memberships. Use this workflow to help you when individuals transition from one job responsibility to another within your organization. You must have the Transform a User role or a role that contains the appropriate powers to transform user accounts. This function can only be done from Delegation and Configuration console via the Account and Resource Management node.

To transform a user account:

1. In the left pane, expand **All My Managed Objects**.

2. To specify the user account you want to manage, execute a **Find Now** operation to locate and then select the user object.

3. Click **Tasks** > **Transform**.

4. Review the Welcome window, and then click **Next**.

5. On the Select User Template window, use **Browse** to select the appropriate subtractive template user.

6. If you want to review the properties of the subtractive template user account, click **View**.

7. Use **Browse** to select the appropriate additive template user.

8. If you want to review the properties of the additive template user account, click **View**.

9. If you have the appropriate powers, you can check **Change other properties of the user** and select properties to modify. Click **Next** to navigate through the properties available.

10. Click **Next**.

11. Review the Summary window, and then click **Finish**.

1.3.2. Managing Groups

As an assistant administrator, you can use DRA to manage groups and modify group properties. Groups enable you to give specific permissions to a defined set of user accounts. Groups let you control which data and resources a user account can access in any domain.

You can manage groups of any type and scope. For example, you can nest groups, allowing one group can inherit permissions from another group. You can also effectively control group memberships across domains by adding groups from trusted domains to other groups in the managed domain and by managing temporary group assignments.

To learn more about managing groups, see the following topics:

- Group Management Tasks

- Managing Temporary Group Assignments in the Delegation and Configuration Console

- Managing Temporary Group Assignments in the Web Console

Group Management Tasks

This section guides you through administering groups in the Delegation and Configuration console via the Account and Resource Management node. With the appropriate powers, you can perform various group management tasks, such as modifying group memberships. If you select multiple groups, you can perform selected tasks in one operation, such as deleting, moving, or adding members to a group. The Tasks menu indicates which tasks you can perform when you select single or multiple groups.

Add accounts to groups

You can add user accounts, contacts, and computers to a managed group.

> **Note**
>
> This task adds multiple accounts to a selected group. You can add a single account to a group by selecting the appropriate account and then clicking Add to groups on the Tasks menu.
>
> If adding an account to another group increases your powers for the account, DRA does not permit you to add the account.

Add groups to other groups

You can nest groups by adding a group to another managed group. When a group is nested in another group, the child group can inherit permissions from the parent group

> **Note**
>
> If adding a group to another group increases your powers for the source group, DRA does not permit you to add the group.

Modify group properties

You can modify properties for local and global groups. The powers you have determine which properties you can modify for a group in the managed domain or managed subtree. If you installed Exchange and enabled Microsoft Exchange support, you can modify distribution list properties while managing groups.

Create a group

You can create a group in the managed domain or managed subtree. You can also modify properties, such as group members, for the new group.

> **Note**
>
> - Your company may have a naming convention enforced through policy that determines the name you can assign to the new group.
>
> - By default, DRA places the new group in the Users OU of the managed domain.

Specify group members

You can add or remove user accounts, contacts, computers, or other groups from the managed group. DRA allows you to only remove foreign security principals. You can also view or modify properties of existing group members, except for foreign security principals.

When you remove members from a group, DRA does not delete the objects. When you add members to a group, you must have the power to modify the objects you want to add.

> **Note**
>
> - You cannot add user accounts or groups to any of the Windows special groups (Administrators, Account Operators, Backup Operators, or Server Operators) unless you are a Windows administrator or a member of that specific special group.
>
> - DRA enables you to export the **Members** results as a CSV file. To export the **Members** results from the Web Console, go to **Management** > **Search** and click **Properties**. Navigate to the **Members** tab and click the **Download** icon.The unsaved changes are not exported. Ensure you save any recent changes so they are available in the exported file.

Specify group membership for groups

You can add or remove a group from other groups in the managed domain or managed subtree. You can also view or modify properties of existing groups to which this group belongs.

> **Note**
>
> DRA enables you to export the **Member Of** results as a CSV file. To export the **Member Of** results from the Web Console, go to **Management** > **Search** and click **Properties**. Navigate to the **Member Of** tab and click the **Download** icon. The unsaved changes are not exported. Ensure you save any recent changes so they are available in the exported file.

Configure group membership security permissions

You can set Active Directory security permissions for group memberships. These permissions specify who can view (read) and modify (write) group memberships using Microsoft Outlook. These settings let you more effectively secure distribution lists and security groups in your environment. You cannot modify inherited security permissions.

> **Note**
>
> When you manage group membership security, disabled permissions may indicate inherited permissions.

Configure group ownership

You can set the ownership of any Microsoft Windows distribution or security groups. You can grant the group ownership permission to a user account, group, or contact. Granting group ownership allows the specified user account, group, or contact to modify the membership of this group.

> **Note**
>
> DRA disables the **Manager can update membership list** check box when group membership is hidden from the Microsoft Exchange server. To enable this check box, click **Expose Group Membership** on the Exchange tab of the Group Properties window.

Clone a group

You can clone both local groups and global groups in managed domains. Cloning groups creates new groups of the same type and attributes as the original group. DRA also attempts to add all members from the original group to the new group.

By cloning a group, you can quickly create groups based on other groups with similar properties. When you clone a group, DRA populates the Clone Group Wizard with values from the selected group. You can also modify properties for the new group.

> **Note**
>
> - Your company may have a naming convention enforced through policy that determines the name you can assign to the new group.
>
> - By default, DRA places the new group in the Users OU of the managed domain.

Delete a group

You can delete local and global groups in the managed domain or managed subtree. If the Recycle Bin is disabled for that domain, deleting a group permanently removes the group from Active Directory. If the Recycle Bin is enabled for that domain, deleting a group moves the group to the Recycle Bin and disables the group properties.

For more information on the Recycle Bin, see Managing the Recycle Bin.

> **Caution**
>
> When you create a group, Microsoft Windows assigns a Security Identifier (SID) to that group. The SID is not generated from the group name. Microsoft Windows uses SIDs to record privileges in access control lists (ACLs) for each resource. If you delete a group, you cannot return access capabilities for that group by creating a new group with the same name.

Move a group to another container

You can move a group to another container, such as an OU, in the managed domain or managed subtree.

Expose group memberships in distribution lists

You can expose group memberships in distribution lists for groups in the managed domain or managed subtree.

Hide group memberships from distribution lists

You can hide group memberships in distribution lists for groups in the managed domain or managed subtree.

Managing Temporary Group Assignments in the Delegation and Configuration Console

Temporary group assignments enable you to manage group memberships for users who only need group membership for a specific time period. This section guides you through administering temporary group assignments in the Delegation and Configuration console under **Account and Resource Management**. With the appropriate powers, you can perform tasks such as creating temporary group assignments or removing expired temporary group

assignments.

Assistant administrators can only view temporary group assignments for groups that the assistant administrator has powers to modify group membership for (add or remove members).

You cannot change the associated group or modify the list of users while the temporary group assignment is in the Active state. If you want to modify these items you must cancel the temporary group assignment.

Manage temporary group assignment properties

You can manage properties for temporary group assignments or saved expired temporary group assignments.

If you want to reschedule a temporary group assignment, change the schedule in the assignment's **Properties** and save your changes.

Create a temporary group assignment

You can create a temporary group assignment on the primary and secondary Administration servers.

By default when a temporary group assignment expires, it is deleted after seven days unless you have selected the **Keep this temporary group assignment for future use** option. To change this retention period, right-click the **Temporary Group Assignment** node under All My Managed Objects, select **Properties**, and modify the number of days to retain temporary group assignments.

Manage user accounts in a temporary group assignment

You can add or remove user accounts from temporary group assignments on the primary and secondary Administration servers.

> **Note**
>
> You can only manage user accounts for temporary group assignments that are not yet active.

Delete a temporary group assignment

You can delete any temporary group assignment on the primary and secondary Administration servers.

Managing Temporary Group Assignments in the Web Console

Temporary group assignments enable you to manage group memberships for users who need group membership for a specific time period. If Microsoft Entra ID is configured by the DRA Administrator, you can create temporary group assignments for Entra ID Groups, and add

Azure users, Azure guest users, and synced users to an Azure group membership. In the Web Console, you can create and manage assignments from both DRA primary and secondary servers. However, actions that you can take on existing assignments vary depending on the state the assignment is in.

Assistant administrators can view temporary group assignments only for groups for which they have powers to modify by their ActiveView assignments, such as adding or removing members of the group.

To manage temporary group assignments in the Web Console, navigate to **Tasks** > **Temporary Group Assignments**.

You can perform the following actions:

Create a temporary group assignment

You can create temporary group assignments by using groups for which you have the powers to modify and also specify the domain controller. The target group can be a group from an Azure managed tenant or a group from an Active Directory domain. When the temporary group assignment expires, DRA automatically deletes it after seven days unless you select the option to keep the temporary group assignment for future use.

> **Note**
>
> If the configured temporary group assignment with Azure group membership is modified outside of DRA, the temporary group assignment becomes invalid.

To create a new temporary group assignment:

1. Navigate to **Tasks** > **Temporary Group Assignments**, and click **Create**.

2. Click **Select**, and find the group by executing a Search in the applicable container.

3. If you need to add members to the group, click **Add** under **Members** in the Create Temporary Group Assignment page, locate and use the **Add** ➕ option in the results list to add members to the group.

4. Configure the Schedule.

5. Name the TGA under General Information, and click **Create**.

Search for existing assignments

When you search for existing temporary group assignments (TGA), they are listed in the results based on the status of the assignment, which can include the following states:

- **Pending:** The TGA is scheduled to start in the future. You can perform cancel, delete, and re-schedule.

- **Active:** The TGA has started and added applicable members to the group. You can perform cancel and delete.

- **Active with Error:** The TGA has started, but failed to add all applicable members to the group. You can perform cancel and delete.

- **Completed:** The TGA has expired and removed all applicable members from the group. You can perform delete and re-schedule.

- **Completed with Error:** The TGA has expired, but failed to remove all applicable members from the group. You can perform delete and re-schedule.

- **Canceled:** The TGA was canceled by a user and removed all applicable members from the group. You can perform delete and re-schedule.

- **Canceled with Error:** TGA was canceled by a user, but failed to remove all applicable members from the group. You can perform delete and re-schedule.

- **Error:** TGA failed to add or failed to remove all the members. You can perform delete and re-schedule.

You can filter the results based on these states and other criteria including the assignment name, target group, duration time, and administrator who created the assignment.

View or Modify temporary group assignment properties

You can view or modify any of the temporary group assignments that were defined when the temporary group assignment was created. After executing a search for temporary group assignments, select an assignment to view or modify its properties.

If you want to reschedule a temporary group assignment, change the schedule in the assignment's **Properties** and save your changes. If the assignment is in the Active state, you can only change the end date.

> **Important**
>
> You may not change the associated group or modify the list of users when the temporary group assignment is in the Active state. If you want to modify these items, you must first cancel the assignment.

Cancel a temporary group assignment

You can cancel a temporary group assignment only when it is in one of the following states:

- Active

- Active with Error

- Pending

Delete a temporary group assignment

You can select multiple temporary group assignments and delete them. If the selected temporary group assignments are in the Active, Active with Error, or Pending state, then

the **Cancel** option is also enabled.

1.3.3. Managing Dynamic Distribution Groups

A dynamic distribution group is a mail-enabled Active Directory group object that you can create to expedite the mass sending of email messages and other information.

The membership list for a dynamic distribution group is calculated each time a message is sent to the group, based on the filters and conditions that you define. This differs from a regular distribution group, which contains a defined set of members. When an email message is sent to a dynamic distribution group, it is delivered to all recipients in the organization that match the criteria defined for that group.

DRA supports the following features:

- Audit and UI reporting

- Enumeration support for dynamic distribution groups

- NetIQ Reporting Center (NRC) report for dynamic distribution groups

- Trigger operation support for dynamic distribution groups

- UI extension support for Exchange dynamic distribution groups

Dynamic distribution group tasks:

Create a dynamic distribution group
You can create a dynamic distribution group in the managed domain or managed subtree. You can also modify properties, such as group members, for the new dynamic distribution group.

> **Note**
>
> - Your company may have a naming convention enforced through policy that determines the name you can assign to the new dynamic distribution group.
>
> - By default, DRA places the new dynamic distribution group in the Users OU of the managed domain.

Clone a dynamic distribution group
You can clone both local and global dynamic distribution groups in managed domains. Cloning dynamic distribution groups creates new dynamic distribution groups of the same type and attributes as the original dynamic distribution group.

By cloning a dynamic distribution group, you can quickly create dynamic distribution groups based on other dynamic distribution groups with similar properties. When you clone a dynamic distribution group, DRA populates the Clone Dynamic Distribution Group

Wizard with values from the selected dynamic distribution group. You can also modify properties for the new dynamic distribution group.

Move a dynamic distribution group to another container

You can move a dynamic distribution group to another container, such as an OU, in the managed domain or managed subtree.

Delete a dynamic distribution group

You can delete local and global dynamic distribution groups in the managed domain or managed subtree. If the Recycle Bin is disabled for that domain, deleting a dynamic distribution group permanently removes the dynamic distribution group from Active Directory. If the Recycle Bin is enabled for that domain, deleting a dynamic distribution group moves it to the Recycle Bin and disables the dynamic distribution group's properties.

For more information on the Recycle Bin, see Managing the Recycle Bin.

> **Caution**
>
> When you create a dynamic distribution group, Microsoft Windows assigns a Security Identifier (SID) to that dynamic distribution group. The SID is not generated from the dynamic distribution group name. Microsoft Windows uses SIDs to record privileges in access control lists (ACLs) for each resource. If you delete a dynamic distribution group, you cannot return access capabilities for that dynamic distribution group by creating a new dynamic distribution group with the same name.

Modify dynamic distribution group properties

You can modify properties for local and global dynamic distribution groups. The powers you have determine which properties you can modify for a group in the managed domain or managed subtree.

Specify a filter

A dynamic distribution list's membership is determined by its filter, which you can define.

Specify conditions

Conditions define the criteria that an object must meet to be a member of the dynamic distribution group.

1.3.4. Managing Dynamic Groups

A dynamic group is one whose membership changes based on a defined set of criteria. In DRA, you can create dynamic groups without having an Exchange environment. The membership filters used to manage dynamic groups in Active Directory are unique to DRA.

The DRA Administrator configures the domain refresh schedule for dynamic groups in the Delegation and Configuration Console. New members are dynamically added to the group when one or more user properties that match the group's Member Filter criteria are updated and then a refresh occurs. In like manner, a member may be dynamically removed from the group when matching properties are changed or removed from the user.

Scenario Example

The graphic below describes a typical use for an Active Directory dynamic group. There are three dynamic groups in the graphic. Each group has a set of criteria that determines who can be added to the group and who can not. Each group controls access to a specific set of files, folders, and applications.

> **Tip**
>
> You can create a *static member list* that contains permanent members of the dynamic group; you can also create an *excluded member list* that denies those users membership in the dynamic group.
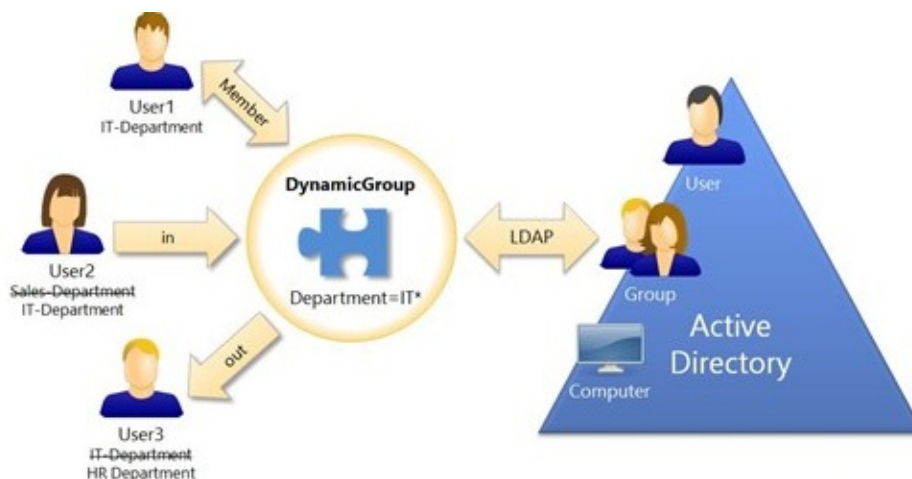
User2 recently joined the IT department. When the IT department's dynamic group is refreshed, she will be added to the group. When the Sales department's dynamic group is refreshed, User2 will be removed from its members list.

User3, who has left the IT department for the HR department, will be removed from the IT department dynamic group and added to the HR department dynamic group.

Scenario Preparation

The information below provides an example of the actions you would take in the Web Console to enable the scenario above. You can make an existing group dynamic or create a new dynamic group. For simplicity's sake, we will not add any static or excluded members and we'll make three existing groups dynamic: HR Group, IT Group, and Sales Group.

Setting up the dynamic group:

1. For each group provided above, perform a Search operation with the Group filter enabled to locate the group.

2. Open **Properties** for the group and access the **Dynamic Member Filter** page.

3. Click the **Make group dynamic** slider to enable the feature.

4. Click **Modify** and type or paste the Member Filter criteria in the LDAP query field. In this case we're looking for criteria in the **User** > **Department** property. The examples below show the LDAP criteria we'll use for each group in the scenario example:

   - HR Group: *(&(objectClass=user)(objectCategory=person)(department=HR*))*

   - IT Group: *(&(objectClass=user)(objectCategory=person)(department=IT*))*

   - Sales Group: *(&(objectClass=user)(objectCategory=person)(department=Sales*))*

5. Click **Apply** to save the changes.

Actions taken to dynamically change users' group affiliation in the selected user's properties:

- User2: Changed the **Organization** > **Department** property from "Sales" to IT".

- User3: Changed the **Organization** > **Department** property from "IT" to "HR".

The dynamic changes occur during the scheduled Dynamic Group Refresh or when manually refreshed by the DRA Administrator.

Dynamic Group Tasks

Dynamic group tasks you can execute in the Web Console are described below.

Create a dynamic group

You can create a dynamic group in the managed domain or managed subtree. You can also modify properties, such as group members, for the new dynamic group. To create a new dynamic group, navigate to **Create** > **Dynamic Group** in the Management masthead.

> **Note**
>
> Your company may have a naming convention enforced through policy that determines the name you can assign to the new dynamic group.

Create a filter

The dynamic group uses the **Dynamic Member Filter** to add or remove users from its membership list each time the group is refreshed. For examples of building LDAP and Virtual Attribute queries for the filter, you can reference examples shown in "Advanced Search Queries". While the filter functions as criteria for group membership and not a search, the query examples are still applicable:

- LDAP query examples

- Virtual Attribute query examples

Manage the static member list

Users placed on a dynamic group's static member list become permanent members of the group until you manually remove them. You can modify this list from Dynamic Member Filter property page on a selected user.

When you remove members from a dynamic group, DRA does not delete the objects. When you add members to a dynamic group, you must have the power to modify the objects you want to add.

Manage the excluded member list

Users placed on a dynamic group's excluded member list will not be allowed to join the group until you manually remove them from this list. You can modify this list from the Dynamic Member Filter property page on a selected user.

Clone a dynamic group

You can clone both local and global dynamic groups in managed domains. Cloning dynamic groups creates new dynamic groups of the same type and attributes as the original dynamic group.

By cloning a dynamic group, you can quickly create dynamic groups based on other dynamic groups with similar properties. When you clone a dynamic group, DRA populates the Clone Dynamic Group Wizard with values from the selected dynamic group. You can also modify properties for the new dynamic group.

To clone a dynamic group, select the group in the Search results pane, and click **Clone** on the toolbar.

Move a dynamic group to another container

You can move a dynamic group to another container, such as an OU, in the managed domain or managed subtree.

To move a dynamic group, select the group in the Search results pane, and click **Move**

Objects 🔧 on the toolbar.

Delete a dynamic group

You can delete local and global dynamic groups in the managed domain or managed subtree.

If the Recycle Bin is disabled for that domain, deleting a dynamic group permanently removes it from Active Directory.

If the Recycle Bin is enabled for that domain, deleting a dynamic group moves it to the Recycle Bin and disables the dynamic group's properties. For more information on the Recycle Bin, see Managing the Recycle Bin.

To delete a dynamic group, select the group in the Search results pane, and click **Delete** 🗑 on the toolbar.

> **Caution**
>
> When you create a dynamic group, Microsoft Windows assigns a Security Identifier (SID) to that dynamic group. The SID is not generated from the dynamic group name. Microsoft Windows uses SIDs to record privileges in access control lists (ACLs) for each resource. If you delete a dynamic group, you cannot return access capabilities for that dynamic group by creating a new dynamic group with the same name.

Modify dynamic group properties

You can modify properties for local and global dynamic groups. The powers you have determine which properties you can modify for a group in the managed domain or managed subtree.

To modify properties of a dynamic group, select the group in the Search results pane, and click **Properties** ✏ on the toolbar.

> **Note**
>
> DRA enables you to export the **Members** and **Member Of** results as a CSV file. To export the **Members** or **Member Of** results from the Web Console, go to **Management** > **Search** and click **Properties**. Navigate to the **Members** or the **Member Of** tab and click the **Download** icon.The unsaved changes are not exported. Ensure you save any recent changes so they are available in the exported file.

Add dynamic groups to other dynamic groups

You can nest dynamic groups by adding a dynamic group to another managed dynamic group. When a dynamic group is nested in another dynamic group, the child dynamic group can inherit permissions from the parent dynamic group.

To add a dynamic group to another dynamic group, select the group in the Search results

pane, and click **Add to Groups** on the toolbar.

> **Note**
>
> If adding a dynamic group to another dynamic group increases your powers for the source dynamic group, DRA will not permit you to add the dynamic group.

Configure group membership security permissions

You can set Active Directory security permissions for dynamic group memberships. These permissions specify who can view (read) and modify (write) dynamic group memberships using Microsoft Outlook. These settings let you more effectively secure distribution lists and security dynamic groups in your environment. You cannot modify inherited security permissions.

You can update these settings from the **Membership Security** property page on a selected dynamic group.

> **Note**
>
> When you manage dynamic group membership security, disabled permissions may indicate inherited permissions.

Configure dynamic group ownership

You can grant the dynamic group ownership permission to a user account, group, or contact. Granting dynamic group ownership allows the specified user account, group, or contact to modify the membership of this dynamic group.

You can update these settings from the **Managed By** property page on a selected dynamic group.

Expose dynamic group memberships in distribution lists

You can expose dynamic group memberships in distribution lists for groups in the managed domain or managed subtree.

You can access this option from the **Exchange** drop-down menu on the toolbar for a selected dynamic group.

Hide dynamic group memberships from distribution lists

You can hide dynamic group memberships in distribution lists for groups in the managed domain or managed subtree.

You can access this option from the **Exchange** drop-down menu on the toolbar for a selected dynamic group.

Note

The **Hide Group Membership** option is disabled for Microsoft Exchange 2007 distribution lists.

1.3.5. Managing Contacts

DRA enables you to manage many network objects, including contacts and the associated email addresses. Contacts are available only in mixed mode or native Microsoft Windows domains. Contacts do not have a Security Identifier (SID), as do user accounts and groups. Use contacts to add members to distribution lists or groups without granting them access to the network services.

You can add contacts to security or distribution groups in mixed and native mode domains. Because security groups can be used as distribution lists in Microsoft Windows, you may want to add contacts to these groups. Having a contact in a global security group does not prevent the group from being converted to a universal security group when you migrate to a native mode Microsoft Windows domain.

Modify contact properties

> You can modify contact properties. The powers you have determine which properties you can modify for a contact in the managed domain. If you installed Exchange and enabled Exchange support, you can modify email address properties while managing the contacts.

> **Note**
>
> DRA enables you to export the **Member Of** results as a CSV file. To export the **Member Of** results from the Web Console, go to **Management** > **Search** and click **Properties**. Navigate to the **Member Of** tab and click the **Download** icon. The unsaved changes are not exported. Ensure you save any recent changes so they are available in the exported file.

Create a contact

> You can create contacts in the managed domain or managed subtree. You can also modify properties, enable email and specify email addresses, and specify group memberships for the new contact.

> To create a new contact, navigate to **Management** > **Search**, and select **Contact** in the Create drop-down menu.

Clone a contact

> By cloning a contact, you can quickly create contacts based on other contacts with similar properties. When you clone a contact, DRA populates the Clone Contact Wizard with values from the selected contact. You can also modify properties, enable email and specify email addresses, and specify group memberships for the new contact.

Manage group memberships for contacts

> You can add or remove contacts from a specific group in the managed domain or managed subtree. You can also view or modify properties of existing groups to which this contact belongs.

Move a contact to another OU

You can move a contact to another container, such as an OU, in the managed domain or managed subtree.

Delete a contact

You can delete a contact from the managed domain or managed subtree. If the Recycle Bin is disabled for that domain, deleting a contact permanently removes the contact from Active Directory. If the Recycle Bin is enabled for that domain, deleting a contact moves the contact to the Recycle Bin.

For more information on the Recycle Bin, see Managing the Recycle Bin.

1.3.6. Managing Group Managed Service Accounts

A group Managed Service Account (gMSA) is a managed domain account that you can assign to services on computer resources. You don't have to manually update the password for these accounts in Active Directory the passwords for these accounts are automatically managed by Windows Server.

You can create and manage a gMSA from the DRA Web Console. A group managed service account can be used with multiple computers to run services. Computers using a gMSA request the current password from Active Directory to start services.

With the appropriate powers, you can perform various tasks related to group Managed Service Accounts. Execute a search operation to locate and select the required a gMSA object. After you select one or more objects in the list, the task bar becomes active with options to delete objects, add objects to groups, remove objects from groups, move objects from one container to another, and modify gMSA properties. You can also download search results as a CSV file. Click the options to display their functions.

Create a gMSA

When you create a gMSA, you must specify the host where this account is used and computers objects that can use the account. Computer objects defined in the membership policy can use the gMSA to run services. Alternatively, you can specify a security group that contains a list of computer objects.

To create a new gMSA, navigate to **Management** > **Search**, and select **Group Managed Service Account** in the Create drop-down menu.

Modify gMSA properties

You can modify gMSA properties. The powers you have determine which properties you can modify for a gMSA in the managed domain.

Enable gMSA

Enabling a gMSA allows you to use the gMSA as the login credentials for a computer service. You can enable or disable a gMSA from the Accounts tab.

Manage group memberships for gMSA

You can add or remove group managed service accounts from a specific group in the managed domain or managed subtree.

Move a gMSA to another container

A gMSA is created under the Managed Service Account container in Active Directory by default. You can move a group managed service account from the default container to another container, such as an OU, in the managed domain or managed subtree.

Delete a gMSA

You can permanently delete a group managed service account from the managed

domain or managed subtree.

1.4. Searching for Objects

This chapter contains conceptual and procedural information about the Search and Advanced Search (LDAP search) functionalities.

- Search

- Advanced Search

1.4.1. Search

DRA enables you to search for objects in on-premises Active Directory domains, Microsoft Exchange, and Azure tenants. You can search for users, guest users, groups, and contacts in your Azure tenants, objects such as users, groups, contacts, computers, printers, OUs and group managed service accounts (gMSA) in your Active Directory domains, and objects such as room mailboxes, equipment mailboxes, shared mailboxes, and dynamic distribution groups in Exchange. You can use the various search options for more efficient and effective searches. DRA automatically truncates any leading or trailing spaces from your search input and returns the search results.

> **Note**
>
> To get an accurate return of searched objects when using object type filters, any changes made to the pagination should be made before applying the object type filters and executing the search. Changing the **items per page** setting at the bottom of the Web Console when object type filters are applied is not supported.

To access the search feature in the Web Console, navigate to **Management** > **Search**.

- Using Wild Characters

- Multi-Field Searching

- Adding and Sorting Columns

- Exporting Search Results

Using Wild Characters

DRA supports wildcard characters such as the question mark (?), asterisk (*), or number sign (#) to maximize your search results. Wildcard matching is not case-sensitive.

The following table provides examples of wildcard character specifications and what they match and do not match.

Character	Match Item
Question mark ?	Any one character or one digit
Number sign #	Any one digit
Asterisk *	Any number of characters or digits

Multi-Field Searching

The Multi-Field Match option enables you to search for matches to multiple attributes with a single search. When you search using Multi-Field Match, your search string is compared to multiple attributes such as name, display name, first name, and last name and if the search string matches any of these attributes, the object is returned in the search results.

The Multi-Field Match option only supports the **"begins with"** search criteria.

For example, if you have two users, one whose *display name* is "`Martin Smith`" and the other user whose user principal name is `martha.jones@acme.com`, and if you perform a search using the string "`Mart`" both users would be returned in the search results.

The table below lists the attributes that are searched for each object type:

Object Type	Attributes Searched
Azure Contact	displayName, givenName, mail, mailNickname, surname
Azure Group	displayName, mail
Azure User	displayName, employeeId, givenName, mail, surname, userPrincipalName
Computer	displayName, name, sAMAccountName
Contact	displayName, employeeId, givenName, mail, mailNickname, name, surname
Dynamic Distribution Group	displayName, mail, mailNickname, name
Group	displayName, mail, mailNickname, name, sAMAccountName
Group Managed Service Account	displayName, name, sAMAccountName
Organizational Unit	name
Recycle Bin	name, sAMAccountName
User	displayName, employeeId, givenName, mail, mailNickname, name, sAMAccountName, surname

> **Note**
>
> The multi-match feature is not supported on Object Selector searches in the Delegation and Configuration console when adding delegates or permissions for the Exchange objects listed below:
>
> - user mailbox
>
> - mail-enabled user
>
> - mail-enabled group
>
> - mail-enabled contact
>
> - dynamic distribution group
>
> - shared mailbox
>
> - resource mailbox

Adding and Sorting Columns

You can sort the search result objects by any of the following attributes when you click an attribute's column header:

- Alias

- Display Name

- Email

- EmployeeID

- First Name

- Last Name

- Location

- Name

- Pre-Windows 2000 Name

- User Principal Name

To add or remove attribute columns, click the column icon.

Exporting Search Results

DRA enables assistant administrators to export **Search** results to a CSV file. To export the **Search** results from the Web Console, go to **Management** > **Search** and click the **Download** icon.

Note

Only the selected columns are exported. If you want additional data, not currently displayed, add those columns first and then export the **Search** results.

1.4.2. Advanced Search

DRA enables you to perform LDAP and virtual attribute queries in your on-premise Active Directory domains from the Advanced Search page. You can search using an existing query, modify an existing query, create a new query, and save new and modified queries for future use as public or private queries. Use the search filters for more efficient and effective searches.

To access the Advance Search queries feature in the Web Console, navigate to **Management > Advanced Search**.

- Advanced Search Queries

- Managing Advanced Queries

- Exporting Advanced Search Results

Advanced Search Queries

DRA supports both virtual attribute and LDAP queries to search for DRA and Active Directory objects. Virtual attributes can be associated with Active Directory object types such as users, groups, dynamic distribution groups, contacts, computers, and OUs. With a virtual attribute query you can filter the results returned from the LDAP query to return only those results that match the virtual attribute query. The virtual attribute query strings must begin with `(objectCategory=<object type>)`. To perform a virtual attribute query, you must specify strings for both LDAP and virtual attribute queries.

LDAP query examples:

- To search for "all computer objects" in DRA:

  LDAP Query: `(objectCategory=computer)`

- To search for user objects with description "East\West Sales" in DRA:

  LDAP Query: `(&(objectCategory=user)(description=East\5CWest Sales))`

- To search for "all computer objects" in DRA:

  LDAP Query: `(objectCategory=computer)`

  > **Important**
  >
  > The backslash character must be escaped in LDAP filters.
  > Substitute \5C.

- To "list all disabled user objects" in DRA:

LDAP Query: `(&(objectCategory=person)(objectClass=user)`
`(userAccountControl:1.2.840.113556.1.4.803:=2))`

The string `1.2.840.113556.1.4.803` specifies `LDAP_MATCHING_RULE_BIT_AND`. This specifies a bitwise AND of a flag attribute (an integer), such as userAccountControl, groupType, or systemFlags, and a bit mask (like 2, 32, or 65536). The clause is True if the bitwise AND of the attribute value and the bit mask is non-zero, indicating the bit is set.

Virtual Attribute query examples:

- To find all users whose company name is ABC:

  Query: `(&(objectCategory=User)(CompanyName=ABC))`

  The DRA object is "User" and the virtual attribute is "CompanyName" (associated with the user).

- To find all users with the company name ABC in the Storage domain:

  Query: `(&(objectCategory=User)(CompanyName=ABC)(Domain=Storage))`

  The DRA object is "User" and the virtual attributes are "CompanyName" and "Domain" (associated with the user)

- To find all groups with the product name DRA or all users with the company name ABC:

  Query: `(|(&(objectCategory=Group)(ProductGroupName=DRA))(&`
  `(objectCategory=User)(CompanyName=ABC)))`

  The DRA objects are "Group" and "User" and the virtual attributes are CompanyName (associated with the user), ProductGroupName (associated with the group).

- To find all groups whose product name is DRA or all users with the company name ABC in the Storage domain:

  Query: `(|(&(objectCategory=Group)(ProductGroupName=DRA))(&`
  `(objectCategory=User)(CompanyName=ABC)(Domain=Storage)))`

  The DRA objects are "Group" and "User" and the virtual attributes are CompanyName (associated with user), ProductGroupName (associated with group), Domain (associated with user.

Managing Advanced Queries

DRA uses LDAP to support the Advanced Search queries feature. Using advanced queries, you can search for users, contacts, groups, computers, OUs, and any other object that DRA supports. If you have the Execute Saved Advanced Queries power, you can execute advanced queries that are available in the **My Searches** and **Public Searches** lists for any container.

In addition to executing a search with a saved advanced query and viewing its details, with the applicable permissions, you can also do the following with advanced queries from the Advanced Search page:

Create a new query

> Create an advanced query on either the primary Administration server or the secondary Administration server by providing the query string (LDAP and, if applicable, virtual attribute) for the new advanced query. After executing the search, expand the **Search** drop-down menu to save the query to either the My Searches list or the Public Searches list.

Modify a query

> Select an existing advanced query under My Searches or Public Searches and use the **Modify** option to change any of the search criteria. Once you execute the search with the updated search criteria, if desired you can expand the **Search** drop-down menu and select **Save** to save the changes to that query.

Copy a query

> Select an existing advanced query under My Searches or Public Searches and execute the search. After executing the search, you can expand the **Search** drop-down menu and select **Save As** to save the query with a different name.

Customize query results

> DRA provides you with a default set of columns in the search results list. To customize your search results from either a saved or unsaved query, click the **Add/Remove Columns** icon 🔲 on the right side of the page to change how the search results are displayed.

Delete a query

> You can delete any advanced query that is in the **My Searches** list. With applicable permissions, you can also delete advanced queries in the **Public Searches** list. To delete a saved advanced query, select it in the applicable list, and click **Delete** in the Search drop-down menu.

Clear a query

> In the Web Console, you can clear the form fields of a saved or unsaved query to make changes from a clean form. To clear the fields in a query, select **Clear** in the Search drop-down menu.

Exporting Advanced Search Results

DRA enables assistant administrators to export **Advanced Search** results to a CSV file. To export the **Advanced Search** results from the Web Console, go to **Management** > **Advanced Search** and click the **Download** icon.

> **Note**
>
> Only the selected columns are exported. If you want additional data, not currently displayed, add those columns first and then export the **Advanced Search** results.

1.5. Managing Entra ID Objects

This chapter contains conceptual and procedural information for managing Entra ID User Accounts, Entra ID Contacts, and Entra ID Groups in the Web Console. With the appropriate powers, you can perform various Azure object management tasks, such as creating and deleting Azure user account objects.

You can execute most of the tasks for Entra ID Objects from the **Management** > **Search** tab in the Web Console by searching for objects in one of the following nodes:

- All My Managed Objects

- All My Managed Tenants

- A sub-node of All My Managed Tenants

Topics include the following:

- Managing Entra ID User Accounts

- Managing Entra ID Guest User Accounts

- Managing Entra ID Groups

- Managing Entra ID Contacts

- Managing an online shared mailbox

1.5.1. Managing Entra ID User Accounts

As an assistant administrator, you can use DRA to manage Entra ID User Accounts and modify Azure user account properties when Microsoft Entra ID is configured by the DRA Administrator. An Azure user account is indicated in the Web Console by this icon .

Execute a search operation to locate and select the required Azure user object. After you select one or more objects in the list, the taskbar becomes active with options such as delete, allow, block, password reset, and modify properties. You can also download search results as a CSV file. Click the options to display their functions.

Create an Azure user account

You can create Entra ID User Accounts in Microsoft Entra ID. You can also enable email and specify group memberships for the new account.

Modify Azure user account properties

You can manage the properties of Entra ID User Accounts in Microsoft Entra ID.The powers you have determine which properties you can modify for an Azure user account. If the Azure user account has an Office 365 mailbox or the Azure user account is mail-enabled, you can manage mailbox-related and mail-related properties for the Azure user account. You can manage mailbox policies, set delivery restrictions and options, set storage limits, delegate mailbox permissions, place litigation on hold, manage email addresses and so on.

> **Note**
>
> - You can update the Mobile Phone, Office Phones, and Alternate Email properties only for Azure users who are non-administrators. For more information, see Update User in the Microsoft Documentation site.
>
> - DRA enables you to export the **Member Of** results as a CSV file. To export the **Member Of** results from the Web Console, go to **Management** > **Search** and click **Properties**. Navigate to the **Member Of** tab and click the **Download** icon. The unsaved changes are not exported. Ensure you save any recent changes so they are available in the exported file.

Allow Sign-In Azure user account

You can enable an Azure user account for signing in to Microsoft Entra ID.

Block Sign-In Azure user account

You can block an Azure user account from signing in to Microsoft Entra ID.

Reset an Azure user account password

You can reset the password for an Azure user account in Microsoft Entra ID and choose whether DRA generates a new password for the account.

Delete an Azure user account

You can delete an Azure user account from Microsoft Entra ID, but it cannot be restored from DRA.

> **Note**
>
> You can delete only those Azure users who are non-administrators. For more information, see Delete a User in the Microsoft Documentation site.

Specify an Azure group membership for Entra ID User Accounts

You can add or remove Entra ID User Accounts from a specific Azure group in Microsoft Entra ID.

1.5.2. Managing Entra ID Guest User Accounts

As an assistant administrator, you can invite external users or guest users to collaborate and share applications in Microsoft Entra ID. Guest users can sign into Microsoft Entra ID using their credentials to access applications that you have shared with them.

Execute a search operation to locate and select the required Azure guest user object. After you select one or more objects in the list, the taskbar becomes active with options such as delete, block sign-in, add to groups, resend an invitation, and modify properties.

Invite an Azure guest user

To invite a guest user to Microsoft Entra ID, navigate to **Create** > **Invite Azure User** in the Management masthead. When you invite a guest user to Microsoft Entra ID, DRA sends an email invitation to the guest user and creates a user account for the guest user in Microsoft Entra ID. An Azure guest user account is indicated in the Web Console by this icon .

> **Note**
>
> The redirect URL and the invitation message are configured by the DRA Administrator in the Delegation and Configuration Console for each managed tenant. You can customize this message as necessary when you invite the user.

An Azure guest user must accept the invitation to start accessing the applications that you have shared. You can view the status of the invitation in the **Guest Info** tab. On accepting the invitation, the user is redirected to the URL that is specified in the **Redirect URL** field, where the Azure guest user can log in using their credentials.

Re-invite an Azure guest user

If the guest user has not accepted the invitation, you can resend the invitation.

To re-invite a guest user:

1. Execute a search operation to locate and select the required Azure guest user object.

2. Select **Account** > **Resend Invite**.

Modify Azure guest user account properties

You can manage the properties of Entra ID Guest User Accounts in Microsoft Entra ID. You can specify whether to hide the email address from appearing in the address list and add alternate email addresses.

Allow Sign-In for an Azure guest user account

You can enable an Azure guest user account for signing in to Microsoft Entra ID.

Block Sign-In for an Azure guest user account

You can block an Azure guest user account from signing in to Microsoft Entra ID.

Delete an Azure guest user account

You can delete an Azure guest user account from Microsoft Entra ID, but it cannot be restored from DRA.

Specify an Azure group membership for Entra ID Guest User Accounts

You can add or remove Entra ID Guest User Accounts from a specific Azure group in Microsoft Entra ID.

Assign licenses to Entra ID Guest User Accounts

When you add an Azure guest user account to a group that is associated with an Office 365 policy, DRA automatically assigns the relevant Office 365 license to the Azure guest user.

Add Entra ID Guest User Accounts to temporary group assignments

You can add or remove Entra ID Guest User Accounts from temporary group assignments from the **Tasks** tab in the masthead on both primary and secondary Administration servers.

1.5.3. Managing Entra ID Groups

As an assistant administrator, you can use DRA to manage Entra ID Groups when Microsoft Entra ID is configured by the DRA Administrator. Entra ID Groups enable you to give specific permissions to a defined set of user accounts. Entra ID Groups let you control which data and resources a user account can access in any tenant.

Execute a search operation to locate and select the required Azure group object. After you select one or more objects in the list, the taskbar becomes active with options to delete objects, add objects to groups, remove objects from groups, add groups to other groups, remove groups from existing groups, and modify group properties. Click the options to display their functions.

> **Note**
>
> Supported Members: Azure group members can be Azure users, Entra ID Groups, Entra ID Contacts, synced users, synced contacts, and synced groups.

The following Azure group types are supported:

- Distribution List

- Mail-enabled Security

- Office 365

- Security

Add accounts to Entra ID Groups

You can add user accounts, contacts, and groups both on-premises and Azure to an Azure managed group.

This task adds multiple accounts to a selected group. You can add a single account to a group by selecting the appropriate account.If adding an account to another group increases your powers for the account, DRA does not permit you to add the account.

Nest groups in Azure

You can nest groups by adding other groups (both on-premises and Azure) to a managed Azure group. When a group is nested in an Azure group, the child group inherits permissions from the parent group.

If adding a domain or Azure group to another Azure group increases your powers for the source group, DRA does not permit you to add the group.

Create an Azure group

You can create an Azure group in Microsoft Entra ID. You can also modify properties, such as adding Azure group members to the new group.

If an owner is not specified, by default DRA provides an Azure tenant access account as the owner.

Modify Azure group properties

The powers you have determine which properties you can modify for a group in Microsoft Entra ID. If the Exchange Policy is enabled, you can manage Exchange properties for mail-enabled Entra ID Groups such as Office 365 group, mail-enabled security group, and distribution list. Depending on the group type, you can manage email addresses for the group, specify who can send email to the group, specify users who can send emails on behalf of the group, set email approval options, and so on.

> **Note**
>
> DRA enables you to export the **Members** and **Member Of** results as a CSV file. Navigate to the **Members** or the **Member Of** tab and click the **Download** icon. The unsaved changes are not exported. Ensure you save any recent changes so they are available in the exported file.

Configure Azure group ownership

You can set the ownership of any groups. You can grant the group ownership permission to a user account or group. Granting group ownership allows the specified user account or group to manage the group including membership.

Delete an Azure group

You can delete Entra ID Groups from Microsoft Entra ID, but they cannot be restored from DRA.

1.5.4. Managing Entra ID Contacts

Entra ID Contacts are mail-enabled objects containing an external email address. As an assistant administrator, you can use DRA to manage Entra ID Contacts and modify Azure contact properties when Microsoft Entra ID is configured by the DRA Administrator.

Execute a search operation to locate and select the required Azure contact object. After you select one or more objects in the list, the taskbar becomes active with options to delete objects, add objects to groups, remove objects from groups, and modify contact properties. You can also download search results as a CSV file. Click the options to display their functions.

Create an Azure contact

You can create an Azure contact in the managed tenant and specify contact information and email addresses for the new Azure contact.

Modify Azure contact properties

You can modify Azure contact properties. The powers you have determine which properties you can modify for an Azure contact in the managed tenant. If Exchange Policy is enabled, you can manage mail-related properties such as set delivery restrictions for messages, specify who can send messages on behalf of this Azure contact, specify whether the Azure contact is visible in the address list and so on.

Enable message moderation

You can set options for moderating messages sent to an Azure contact. When you enable moderation, messages sent to the Azure contact will be approved by a moderator that you define before the messages are delivered. You can also specify users and groups who are exempted from the approval process.

Manage group memberships for Entra ID Contacts

You can add or remove Entra ID Contacts to mail-enabled security groups and distribution lists.

> **Note**
>
> DRA enables you to export the **Member Of** results as a CSV file. Navigate to the **Member Of** tab and click the **Download Saved Membership** icon. The unsaved changes are not exported. Ensure you save any recent changes so they are available in the exported file.

Delete an Azure contact

You can delete Entra ID Contacts from Microsoft Entra ID, but they cannot be restored from DRA.

1.5.5. Managing an online shared mailbox

Managing an online shared mailbox

As an assistant administrator, you can use DRA to manage Online Shared Mailbox and modify Online Shared Mailbox properties when Microsoft Entra ID is configured by the DRA Administrator.

Execute a search operation to locate and select the required Online Shared Mailbox object. After you select one or more objects in the list, the taskbar becomes active with options such as create, delete and modify properties. You can also download search results as a CSV file. Click the options to display their functions.

Create an online shared mailbox

You can create an Online Shared Mailbox with mailbox delegations in Microsoft Entra ID.

Modify an online shared mailbox properties

You can manage the properties of Online Shared Mailboxes in Microsoft Entra ID.

The powers you have determine which properties you can modify for an Online Shared Mailbox. You can manage mailbox policies, set delivery restrictions and options, set storage limits, delegate mailbox permissions, place litigation on hold, manage email addresses and so on.

Delete an online shared mailbox

You can delete an Online Shared Mailbox from Microsoft Entra ID, but it cannot be restored from DRA.

1.6. Managing Exchange Mailboxes and Public Folders

Using DRA you can manage Microsoft Exchange mailboxes as an extension of user account properties. This integration enables you to simplify your administration workflows so you can effectively administer Exchange properties. You can also link mailboxes from the user account and Exchange account forests and manage resource mailboxes, shared mailboxes, and public folders.

Table 6-1 Types of Exchange Mailboxes Supported in DRA

Microsoft Mailbox Objects	Object type	Mailbox Type	Operations supported in DRA	Supported from DRA Version
On-Prem User Mailbox	User	Mailbox	Search/CRUD	10.1
Online User Mailbox	User	Online	Search/CRUD	10.1
On-Prem Shared Mailbox	Shared Mailbox	-	Search/CRUD	10.1
On-Prem Shared Mailbox	User	Mailbox	Search/CRUD	10.1
On-Prem Room Mailbox	Room Mailbox	-	Search/CRUD	10.1
On-Prem Room Mailbox	User	Mailbox	Search/CRUD	10.1
On-Prem Equipment Mailbox	Equipment Mailbox	-	Search/CRUD	10.1
On-Prem Equipment Mailbox	User	Mailbox	Search/CRUD	10.1
Entra ID User Mailbox	Entra ID User	Mailbox, Online	Search/CRUD	10.1
Provision Remote User Mailbox	User	Mailbox, Remote	Search/CRUD	10.2.1

Microsoft Mailbox Objects	Object type	Mailbox Type	Operations supported in DRA	Supported from DRA Version
Provision Remote Shared Mailbox	Shared	Remote	Search/CRUD	10.2.1
Provision Remote Shared Mailbox	User	Mailbox, Remote	Search/CRUD	10.2.2
Provision Remote Room Mailbox	Room Mailbox	Online	Search/RUD	10.2.2
Provision Remote Room Mailbox	User	Online	Search/RUD	10.2.2
Provision Remote Equipment Mailbox	Equipment Mailbox	Online	Search/RUD	10.2.2
Provision Remote Equipment Mailbox	User	Online	Search/RUD	10.2.2
Migrated Remote User Mailbox	User	Mailbox, Remote	Search/RUD	10.2.3
Migrated Remote Shared Mailbox	Shared	Remote	Search/RUD	10.2.3
Migrated Remote Shared Mailbox	User	Mailbox, Remote	Search/RUD	10.2.3
Migrated Remote Room Mailbox	Room Mailbox	Online	Search/RUD	10.2.3
Migrated Remote Room Mailbox	User	Online	Search/RUD	10.2.3
Migrated Remote Equipment Mailbox	Equipment Mailbox	Online	Search/RUD	10.2.3
Migrated Remote Equipment Mailbox	User	Online	Search/RUD	10.2.3
Online Shared Mailbox	Online Shared Mailbox	-	Search/CRUD	10.3

Microsoft Mailbox Objects	Object type	Mailbox Type	Operations supported in DRA	Supported from DRA Version
Entra ID/Cloud Room Mailbox	Entra ID User	-	Search/RUD	-
Entra ID/Cloud Equipment Mailbox **	Entra ID User	-	Search/RUD	

> **Note**
>
> CRUD: C- Create, R-Read, U- Update, D- Delete.
>
> **Objects are currently not supported; only basic Entra ID properties can be updated.

Managing Mailbox Tasks in the Delegation and Configuration Console

When using the ARM node, you execute applicable mailbox tasks from the **Exchange Tasks** tab in the object's properties, which is also accessible from the **Tasks** or the right-click menu for a selected object. Generally, you select the **All My Managed Objects** node and execute a **Find Now** operation to locate and select the desired object.

Managing Mailbox Tasks in the Web Console

When using the Web Console, you execute the applicable mailbox tasks below from the **Management** > **Search** tab. Generally, you execute a search operation to locate and select the required mailbox object. After you select one or more objects in the list, the taskbar becomes active. Click the options to display their functions.

See the following topics:

- User Mailboxes

- Remote Mailboxes

- Resource Mailboxes

- Shared Mailboxes

- Linked Mailboxes

- Office 365 Mailboxes

- Public Folders

1.6.1. User mailboxes

You can manage Microsoft Exchange mailboxes for user accounts in the managed domain or managed subtree. Each aspect of managing Microsoft Exchange mailboxes requires different powers. The powers you have control which mailbox properties you can modify, or whether you can create, clone, view, or delete Microsoft Exchange mailboxes. You can also manage mailbox rights and permissions associated with a user account, allowing you to control the security of your Microsoft Exchange environments. If you do not have the required power to modify a tab or field for the selected mailbox, DRA disables the tabs and fields that you cannot modify.

In addition to the tasks defined below, user accounts may have options enabled in the object properties by the DRA Administrator to configure settings for Skype and Skype Online. Skype can be configured from user accounts in both the Delegation and Configuration Console and the Web Console. Skype Online can only be configured from the Web Console.

Create a mailbox

You can create a Microsoft Exchange mailbox for an existing user account. You can also modify properties for the new mailbox.

> **Note**
>
> When you create a mailbox, Exchange generates the necessary proxy strings based on your Exchange policy settings. Microsoft Exchange also generates default proxy strings. As a result, when you view the properties of the newly created mailbox, you see both types of proxy strings.

Clone a user account

When you clone a user account, any groups that the user is a member of are automatically added to the new user account, saving you time in configuring the new account. You can add or remove groups from the new account, enable email, and make any other property configurations as you would with any new account.

> **Note**
>
> When you clone an InetOrgPerson object, you create a user account.

Move a mailbox

You can move a Microsoft Exchange mailbox for a user account to another mailbox store or Microsoft Exchange server.

Modify mailbox properties

You can modify properties for Microsoft Exchange mailboxes as you manage the associated user accounts. The powers you have determine the mailbox properties you can modify.

> **Note**
>
> You cannot modify the mailbox properties of user accounts managed on member servers.

Configure mailbox security permissions

You can specify which user accounts, groups, or computers you want to grant or deny the ability to send and receive email using a specific Microsoft Exchange mailbox. These settings let you more effectively secure your Exchange environment. You cannot modify inherited security permissions.

> **Note**
>
> When you manage mailbox security, disabled permissions may indicate inherited permissions.

Remove mailbox security permissions

You can remove mailbox security permissions from a user account, group, or computer associated with a Microsoft Exchange mailbox. Removing mailbox security permissions prevents the user account, group, or computer account from sending and receiving email through the specified mailbox. You cannot remove inherited security permissions.

Configure mailbox rights

You can grant or deny other user accounts, groups, or computers rights to a specific Microsoft Exchange mailbox. These settings let you more effectively secure your Exchange environment. You cannot modify inherited mailbox rights.

> **Note**
>
> When you manage mailbox rights, disabled permissions may indicate inherited permissions.

Remove mailbox rights

You can remove mailbox rights from user accounts, groups, or computers associated with a specific Microsoft Exchange mailbox. Removing mailbox rights prevents the user account, group, or computer account from using the specified mailbox. You cannot remove inherited mailbox rights.

Delete a mailbox

You can delete a mailbox associated with a user account in the managed domain or managed subtree. Deleting a mailbox also deletes all messages in the mailbox.

Add or modify an email address

You can specify email addresses for mailboxes associated with user accounts in your managed domain or managed subtree. You can also assign email addresses to user

accounts who do not yet have mailboxes. When managing Microsoft Exchange mailboxes, you can add only the email address types defined by your proxy generation policies.

Specify a reply address

You can set reply addresses for a mailbox associated with a user account in the managed domain or managed subtree. You can set several reply addresses for a mailbox. However, you cannot set more than one email address type as a reply address. For example, you cannot specify more than one Internet address as a reply address.

Delete an email address

You can delete an email address by removing the address from the mailbox.

Specify delivery options

You can specify which mailboxes the user can use to send messages, set forwarding options, and specify recipient limits.

Specify delivery restrictions

By setting delivery restrictions, you can limit the size of incoming and outgoing messages and the acceptance of incoming messages for a specific mailbox.

Specify storage limits

You can specify storage limits, such as warnings based on the size of a mailbox. You can also specify retention times for deleted items.

Check mailbox move status

You can check the status of mailbox moves and take actions on them, such as clearing the status, canceling a move, and resuming a move that has been interrupted.

1.6.2. Remote mailboxes

With DRA 10.2.1 you can create, configure, and delete remote mailboxes in your Exchange hybrid organization. You can manage the following types of remote mailboxes from the Web Console:

- Remote user mailbox

- Remote shared mailbox

For a remote mailbox, a remote routing address is required. If you have configured a remote routing address generation rule, DRA generates the remote routing address based on the rule when you create a remote mailbox. You can change this generated remote routing address as needed. For information about the remote routing address rule, see "Configuring a Remote Routing Address Policy".

A remote mailbox is indicated in the Web Console by this icon . The existing DRA powers for managing on-premises Exchange mailboxes also apply to remote mailboxes. The powers you have determine the remote mailbox properties that you can modify and the tasks that you can perform on remote mailboxes. If you do not have the necessary power to modify a tab or field for the selected remote mailbox, DRA disables the tabs and fields.

Remote User Mailboxes

A remote user mailbox is a user account in the managed hybrid domain (on-premises Active directory) with an associated mailbox in the cloud-based service or the Exchange Online environment.

Create a remote user mailbox
When you create a user account in a hybrid domain of the on-premises Active Directory, you can create a remote mailbox for that user. On the Mailbox tab, turn on the **Create Mailbox** toggle and select Remote Mailbox to create a remote mailbox for the user. You must specify a licensing group that is configured with an office 365 policy and a remote routing address for the mailbox.

You can also create an archive mailbox for the user's remote mailbox. Select the user account for which you want to create an archive mailbox, and then click **Exchange** > **Create Archive Mailbox**.

Create a remote user mailbox for an existing user account
If a user account does not have a mailbox, you can create a remote mailbox by selecting **Exchange** > **Create Mailbox**. On the Create Mailbox page, select **Remote Mailbox**, and specify a licensing group that is configured with an office 365 policy and a remote routing address for the mailbox.

View and configure remote user mailbox properties

After you create a remote user mailbox, you can view and configure the following mailbox properties:

- Message delivery restrictions

- Storage limit for the remote mailbox and archive mailbox

- Deleted item retention

- Email addresses

- Advanced message settings

- MailTip

- Litigation hold

- Mailbox permissions

- Message forwarding

> **Note**
>
> You can only view the mailbox statistics.

For more information, see Configure Remote Mailbox Properties.

Delete a remote user mailbox or an archive mailbox

When you delete a user account with a remote mailbox from the on-premises Active Directory, you also delete the remote mailbox from the cloud-based service. If the Recycle Bin is enabled for the hybrid domain, deleting a remote user mailbox moves it to the Recycle Bin. The deleted user account with the remote mailbox can be restored.

To delete a remote mailbox from the cloud-based service, you must disable the remote mailbox by selecting **Exchange** > **Delete Mailbox.** If an archive mailbox exists, it is also deleted. Deleting a remote mailbox from the cloud-based service does not delete the associated user account in the on-premises Active Directory.

You can also delete only the archive mailbox while keeping the mailbox in the cloud-based service.

Remote Shared Mailboxes

A remote shared mailbox is a disabled user account in the on-premises Active Directory with an associated mailbox in the cloud-based service or Exchange Online. You can create a remote shared mailbox without assigning a licensing group.

> **Note**
>
> If you wish to assign licenses to a remote shared mailbox after it has been created, you must include it in a group that is associated with an Office 365 policy by using the Member Of properties page.

Create a remote shared mailbox

When you create a shared mailbox in the on-premises Active Directory, you can choose to create the shared mailbox as a remote mailbox. On the **General** tab, under **Mailbox Options**, select **Remote Mailbox**. Specify a remote routing address and Send As permission for the mailbox.

To create an archive mailbox for the remote shared mailbox, select the remote shared mailbox, and then click **Exchange** > **Create Archive Mailbox**.

View and configure remote shared mailbox properties

After you create a remote shared mailbox, you can view and configure the following mailbox properties.

- Message delivery restrictions

- Storage limit for the remote mailbox and archive mailbox

- Deleted item retention

- Email addresses

- Advanced message settings

- MailTip

- Litigation hold

- Mailbox permissions

- Message forwarding

> **Note**
>
> You can only view the mailbox statistics.

For more information, see Configure Remote Mailbox Properties.

Delete a remote shared mailbox or an archive mailbox

When you delete a remote shared mailbox from the on-premises Active Directory, you permanently delete the shared mailbox account from the on-premises Active Directory as well as the associated mailbox from the cloud-based service. If an archive mailbox exists, it is also deleted. If the Recycle Bin is enabled for the hybrid domain, deleting a remote shared mailbox moves it to the Recycle Bin. The deleted remote shared mailbox

can be restored.

You can also delete only the archive mailbox while keeping the mailbox in the cloud-based service.

Configure Remote Mailbox Settings

You can configure the following settings for a remote mailbox:

Message delivery restrictions

Limit the size of incoming and outgoing messages for a specific object, as well as accept or reject incoming messages.

Storage limit for the remote mailbox

Limit the size of the remote mailbox and prevent the sending and receiving of messages when the remote mailbox reaches the configured size. You can also configure warnings to be sent when the remote mailbox's size exceeds the predefined limit.

Storage limit for the remote archive mailbox

Set a storage limit for the archive mailbox and configure warnings to be sent when an archive mailbox's size exceeds a predefined limit.

Deleted item retention

Use the mailbox store's settings to retain deleted mailbox objects or to specify how long the deleted mailbox objects are retained before they are permanently deleted and cannot be restored.

Email addresses

Modify existing addresses or create new addresses for the remote mailbox including the primary email address. You can also specify whether to apply email address policies to the remote mailbox and update the remote routing address for the user's remote mailbox.

Advanced message settings

Specify whether the user is visible in the address list and prevent the remote mailbox from sending messages to an X400 type email address.

MailTip

Add informational text that you want to be displayed when a message is sent to users.

Litigation hold

Set a litigation hold on a remote mailbox to preserve all mailbox content, including deleted items and original versions of modified items. Placing a user's remote mailbox on litigation hold also preserves content, if it exists, in the archive mailbox as well. The hold can last for a specified period, or until you remove the Litigation Hold from the remote mailbox.

Mailbox permissions

Delegate the remote mailbox to other users and groups who can use the mailbox to read and send messages. You can delegate three types of permissions to users: send as, send on behalf of, and full access.

Message forwarding

Configure the remote mailbox to forward messages sent to it to another mailbox and specify the maximum number of recipients to whom a message can be forwarded.

1.6.3. Resource mailboxes

Microsoft Exchange's resource mailbox feature enables you to create a mailbox that represents a resource such as a conference room so that you can reserve it by sending it a meeting invitation, just as you would a person. DRA contains a set of roles, powers, and policies that allow you to manage your resource mailboxes efficiently.

DRA has interface extension support for resource mailboxes as well as support for generating audit or user interface reports. Support for ADSI scripts is also integrated into DRA.

Create a resource mailbox

You can create resource mailboxes in the managed domain or managed subtree.

Move a resource mailbox to another container

You can move a resource mailbox to another container, such as an OU, in the managed domain or managed subtree.

Move a resource mailbox to another mailbox store or Exchange server

You can move a resource mailbox to another mailbox store or Microsoft Exchange server.

Clone a resource mailbox

By cloning a resource mailbox, you can quickly create other resource mailboxes with similar properties. When you clone a resource mailbox, DRA populates the Clone Resource Mailbox Wizard with values from the selected resource.

Rename a resource mailbox

You can rename resource mailboxes in the managed domain or managed subtree. Changing the user logon name also changes the name of the mailbox associated with the user account.

Add a resource mailbox to a group

You can add resource mailboxes to a specific group in the managed domain or managed subtree.

Delete a resource mailbox

You can delete a resource mailbox in the managed domain or managed subtree. Deleting a resource mailbox also deletes all messages in the mailbox and any disabled user objects associated with the resource mailbox. If desired, you can override the deletion of disabled user objects when you delete the mailbox. If you delete a user object associated with a resource mailbox the resource mailbox is also deleted.

Restore a deleted resource mailbox

You can restore a resource mailbox that was deleted if the Recycle Bin from that domain is enabled.

Modify resource mailbox properties

You can manage the properties of resource mailboxes in the managed domain or managed subtree. The powers you have determine which properties you can modify.

Note

DRA enables you to export the **Member Of** results as a CSV file. To export the **Member Of** results from the Web Console, go to **Management** > **Search** and click **Properties**. Navigate to the **Member Of** tab and click the **Download** icon. The unsaved changes are not exported. Ensure you save any recent changes so they are available in the exported file.

1.6.4. Shared mailboxes

Shared mailboxes are useful to Helpdesk administrators and technical support staff, because all responses can be configured to go into a single mailbox that multiple users can access. The mailbox must be in a DRA managed domain with the Exchange Policy enabled, and you must have powers delegated to you to manage shared mailboxes.

When you create a shared mailbox, there are two types of permissions you can delegate to users: Send As and Full Access. Send As provides permission to read and send emails. You can delegate permissions to both user and group objects. You can also specify delivery restrictions, delivery options, storage limits, folder permissions, and several other options in the object's properties.

> **Note**
>
> You can perform management tasks for shared mailboxes only through the Web Console.

Create a shared mailbox

You can create shared mailboxes in the managed domain or managed subtree.

Move a shared mailbox to another container

You can move a shared mailbox to another container, such as an OU, in the managed domain or managed subtree.

Move a shared mailbox to another mailbox store

You can move a shared mailbox to another mailbox store.

Clone a shared mailbox

By cloning a shared mailbox, you can quickly create other shared mailboxes with similar properties.

Rename a shared mailbox

You can rename shared mailboxes in the managed domain or managed subtree. Changing the user logon name also changes the name of the mailbox associated with the user account.

Delete a shared mailbox

You can delete a shared mailbox in the managed domain or managed subtree. If the Recycle Bin is disabled for that domain, deleting a shared mailbox permanently removes it from Active Directory. If the Recycle Bin is enabled for that domain, deleting a shared mailbox moves it to the Recycle Bin.

Deleting a shared mailbox also deletes all messages in the mailbox and any disabled user objects associated with the shared mailbox. If you delete a user object associated with a shared mailbox the shared mailbox is also deleted.

Restore a deleted shared mailbox

You can restore a shared mailbox that was deleted if the Recycle Bin from that domain is enabled.

Create an archive shared mailbox

You can create archived shared mailboxes in the managed domain or managed subtree.

Delete an archive shared mailbox

You can delete archived shared mailboxes in the managed domain or managed subtree.

Modify shared mailbox properties

You can modify the properties of shared mailboxes in the managed domain or managed subtree. The powers you have determine which properties you can modify.

Note

DRA enables you to export the **Member Of** results as a CSV file. To export the **Member Of** results from the Web Console, go to **Management** > **Search** and click **Properties**. Navigate to the **Member Of** tab and click the **Download** icon. The unsaved changes are not exported. Ensure you save any recent changes so they are available in the exported file.

1.6.5. Linked mailboxes

Linked mailboxes are useful for large organizational changes that occur during mergers, acquisitions, and company splits, when mailbox migration is common. This feature enables linking mailboxes from different Exchange forests to negate disruption of user email. The mailboxes must be in DRA managed domains with the Exchange Policy enabled, and you must have powers delegated to you to manage linked mailboxes. When you create a linked mailbox, a **Linked Mailbox** tab is added to the properties of the user object.

Linked mailbox management is only supported in the Web Console. You create a linked mailbox from the toolbar of a selected user account. This option is only enabled when the selected user's domain has an external forest trust with other managed domains in DRA. Only disabled user accounts will be listed when searching for an account to link to in another DRA managed domain.

Create a linked mailbox

You can create a linked mailbox from two user accounts selected in different managed Exchange forests.

Delete a linked mailbox

You can delete a linked mailbox from the toolbar of a selected user that has a linked mailbox.

Modify linked mailbox properties

You can modify the properties of a linked mailbox from the **Linked Mailbox** tab in a selected user's properties.

Create a linked archive mailbox

You can create a linked archive mailbox from a selected user that has a linked mailbox.

Delete a linked archive mailbox

You can delete a linked archive mailbox from the toolbar of a selected user that has a linked archive mailbox.

Restore a deleted linked mailbox

You can restore a linked mailbox that was deleted if the Recycle Bin from that domain is enabled.

1.6.6. Office 365 mailboxes

This section contains information for administering Microsoft Office 365 mailboxes in the Delegation and Configuration console via the Account and Resource Management node and in the Web Console. With the appropriate powers, you can perform various user account management tasks, such as placing litigation holds, setting up email forwarding and so on.

> **Important**
>
> DRA manages Office 365 user mailboxes as well as migrated shared, room, and equipment mailboxes. For DRA to manage these mailboxes they must be associated with an on-premises user or Azure user that is managed by DRA. The mailbox properties will be available through the property pages for those associated users.

1. Execute a **Find Now** operation to locate and select the user account.
2. Right-click the user object, and go to **Properties > Litigation Hold**.
3. Select the **Enable Litigation Hold** check box, and do one of the following:
   1. Select the **Indefinite** check box if the duration for the hold is unknown.
   2. Select the **Number of days** check box and provide the value if the required hold duration is
      known

Place a litigation hold

Set a litigation hold on a mailbox to preserve all mailbox content, including deleted items and original versions of modified items. Placing a user's mailbox on litigation hold also preserves content, if it exists, in the user's archive mailbox as well. The hold can last for a specified period, or until you remove the Litigation Hold from the mailbox.

You must have the appropriate Exchange Online license to place a litigation hold. You configure the feature via the **Litigation Hold** tab in the user object's properties.

Delegate mailbox permissions

You can delegate Office 365 mailbox permissions via the Mailbox delegation tab in the user object's properties. There are three types of permissions that you can delegate, send as, send on behalf of, and full access. The types of permission that can be delegated depends upon the receiving object type.

View archive mailbox status

You can view the status of the archive mailbox for a user and the archive mailbox statistics such as storage limit and warning limit. When the archive mailbox exceeds the archive warning limit, the user is notified.

View mailbox usage statistics

You can view the amount of the total mailbox quota that has been used.

Configure message delivery restrictions

By setting delivery restrictions, you can limit the size of incoming and outgoing

messages and accept or reject incoming messages for a specific user.

Configure delivery options

You can configure message forwarding options and specify maximum recipients that a user can send a message to.

Add or remove an email address

You can configure more than one email address for a user mailbox and specify the primary email address. You can also assign email addresses to user accounts that do not have mailboxes.

Hide email address

You can specify whether to hide the email address from appearing in the address list.

Add MailTip

You can add informational text that you want to be displayed when a mail is sent to the user.

Assign policies for mailbox

You can assign a sharing policy, email retention policy, role assignment policy, or address book policy for the mailbox

Placing a Litigation Hold

To set a litigation hold on a mailbox:

1. Execute a **Find Now** operation to locate and select the user account.
2. Right-click the user object, and go to **Properties > Litigation Hold**.
3. Select the **Enable Litigation Hold** check box, and do one of the following:
   1. Select the **Indefinite** check box if the duration for the hold is unknown.
   2. Select the **Number of days** check box and provide the value if the required hold duration is known.

Delegating Mailbox Permissions

The types of permission that can be delegated depends upon the receiving object type:

- Send as
- Send on behalf of
- Full access

To delegate mailbox permissions:

1. Execute a **Find Now** operation to locate and select the user account or group.
2. Right-click the object, and go to **Properties > Mailbox delegation**.
3. In the right pane, do one or more of the following:

- To allow a user or group to send messages using this mailbox, click the plus (+) sign beneath the Send As label and select the appropriate user or group.
- To revoke the ability of a user or group to send messages using this mailbox, select the account and click the delete (x) sign beneath the Send As label.
- To allow a user to send messages on behalf of this mailbox, click the plus (+) sign beneath the Send on Behalf label and select the appropriate user.
- To revoke the ability of a user to send messages on behalf of this mailbox, select the account and click the delete (x) sign beneath the Send on Behalf label.
- To allow a user or a group full access to this mailbox, click the plus (+) sign beneath the Full Access label and select the appropriate user or group.
- To deny a user or a group full access to this mailbox, select the account and click the delete (x) sign beneath the Full Access label.

> **Important**
>
> DRA manages Office 365 user mailboxes as well as migrated shared, room, and equipment mailboxes. For DRA to manage these mailboxes they must be associated with an onpremise user that is managed by DRA. The mailbox properties will be available through the property pages for those associated users.

1.6.7. Public folders

If the DRA Administrator has created Public Folder forests in the DRA managed enterprise and granted you powers to manage public folders in DRA, you will be able to create public folders, modify their properties, and generate change history reports. Creating and modifying public folders can only be done in the Web Console. You can use the search option to search public folders. For information, see Search.

You execute Public Folder tasks from the **Management** > **Public Folders** tab.

Create a public folder

You can create new public folders in specified Public Folder domains, subtrees, and mailboxes through the Web Console. You can use the default mailbox for the selected domain or choose one.

Enable email for a public folder

You can enable email for a public folder using the **Enable Mail** option on the list toolbar. This enables you to associate email addresses with the public folder and modify the public folder's properties.

Disable email for a public folder

You can disable email for a public folder using the **Disable Mail** option on the list toolbar.

Modify public folder properties

After enabling mail on an existing public folder, you can view the folder's statistics, and modify the properties of that public folder. In these properties, you can specify user delivery and restriction options, size limits and quota warnings, mail properties, storage age limits, inclusion of moderators to approve mail, and custom attributes.

> **Note**
>
> You can also update some properties for multiple public folders when more than one is selected, such as storage quotas.

Delete a public folder

You can delete public folders if they do not have any sub-folders and the email option is disabled.

1.7. Managing Resources

DRA enables you to manage resources including computers, printers, and other devices, as well as processes associated with these resources. For example, if you need to start a specific service on a managed computer, you could search for that computer object in DRA, access its services through object properties, and then restart a specific service on that computer from DRA without ever having to log in remotely to that computer.

- Managing Organizational Units (OUs)

- Managing Computers

- Managing Services

- Managing Printers and Print Jobs

- Managing Shares

- Managing Connected Users

- Managing Devices

- Managing Event Logs

- Managing Open Files

1.7.1. Managing Organizational Units (OUs)

This section guides you through administering OUs in the Delegation and Configuration console via the Account and Resource Management node. With the appropriate powers, you can perform various OU management tasks, such as moving an OU to another container.

> **Note**
>
> You can manage OUs only through the Delegation and Configuration Console.

Modifying OU Properties

You can modify properties for OUs. The powers you have determine which properties you can modify for an OU in the managed domain or managed subtree.

Creating an OU

You can create an OU in the managed domain or managed subtree. You can also modify general properties, such as the OU description.

Cloning an OU

You can create a new OU by cloning an existing OU from the managed domain or managed subtree. You can also modify general properties for new OU, such as the OU description. Cloning an OU does not clone the objects contained in the OU.

Opening the Active Directory Tree to an OU Location

You can quickly and easily open the Active Directory tree to the location of a specific OU in the managed domain or managed subtree.

Moving an OU to Another Container

You can move an OU to a different container in the managed domain. When managing a subtree of a domain, you can move OUs within the hierarchy of that subtree.

> **Note**
>
> - If moving an OU to another container increases your powers for the moved OU, DRA does not permit you to move the OU.
>
> - You can also move an OU by dragging it to the new location.

Deleting an OU

You can delete OUs from the managed domain or managed subtree. You can only delete empty OUs. If an OU contains objects, you cannot delete the OU. To delete an OU that contains objects, delete all of the objects first, and then delete the OU.

1.7.2. Managing Computers

DRA enables you to administer computers in the managed domain or managed subtree. For example, you can add or remove computer accounts in the managed domains, as well as manage the resources on each computer. When you add a computer to a domain, DRA creates a computer account in that domain for that computer. You can then connect the computer in that domain and configure the computer to use that computer account. You can also view and modify the properties of computer accounts. DRA also lets you shut down a computer and synchronize domain controllers in a managed domain.

> **Note**
>
> - You can manage computers only through the Delegation and Configuration Console.
>
> - You cannot manage hidden domain controllers. The domain cache does not include hidden domain controllers. Therefore, DRA does not display hidden domain computers in lists or property windows

Specify group membership for computers

You can add or remove computers from a specific group in the managed domain or managed subtree. You can also view or modify properties of existing groups to which this computer belongs.

> **Note**
>
> DRA enables you to export the **Member Of** results as a CSV file. To export the **Member Of** results from the Web Console, go to **Management** > **Search** and click **Properties**. Navigate to the **Member Of** tab and click the **Download** icon. The unsaved changes are not exported. Ensure you save any recent changes so they are available in the exported file.

Manage computer account properties

You can manage computer account properties. The powers you have determine which properties you can modify for a computer in the managed domain or managed subtree.

Add a computer to a domain

You can add a computer to a managed domain or managed subtree by creating a new computer account.

Remove a computer from a domain

You can remove a computer from a managed domain or managed subtree by deleting the computer account.

Move a computer

You can move a computer to another container, such as an OU, in the managed domain

or managed subtree.

Shut down or restart a computer

You can shutdown and restart a computer immediately or at a set date and time.

Reset the Administrator account password

To reset the administrator account password for a computer, you must have the Reset Password for Local Administrator power or be associated with a role that contains this power. You can reset the administrator password for member servers in your managed domain or managed subtree. You cannot reset the administrator password for a domain controller.

Reset the computer account

You can reset a computer account for member servers in your managed domain or managed subtree. You cannot reset the computer account for a domain controller.

Delete a computer account

You can delete a computer account from the managed domain or managed subtree. If you are managing a Microsoft Windows domain, you can delete computer accounts that contain other objects, such as a shared resource. Enable the **Force Delete** option to delete computer objects from Active Directory. This will also delete child objects, including printers and shared folders. Deleted computers and their associated objects are moved to the DRA Recycle Bin. If the Recycle Bin is disabled upon deletion, the objects are permanently deleted.

> **Note**
>
> You cannot delete computer accounts for member servers in the managed domain or managed subtree.

Disable a computer account

You can disable a computer account in the managed domain or managed subtree. Disabling a computer account prevents users on that computer from logging on to any domain.

Enable a computer account

You can enable a computer account in the managed domain or managed subtree. Enabling a computer account allows users on that computer to log on to any domain.

Manage computer resources

For each computer account in the managed domain or managed subtree, you can manage the associated resources, such as services, shares, devices, printers, and print jobs.

1.7.3. Managing Services

A service is a type of application that gets special treatment from the Windows operating system. Services can run even when no user is currently logged on to a computer. Assistant administrators with the appropriate powers can manage services that are running on computers in the managed domain or managed subtree.

Manage service properties

> You can manage properties for services running on computers in the managed domain or managed subtree. You can manage services while managing other resources for that computer.

Start a service

> You can start a service on any computer in the managed domain or managed subtree.

Start a service with parameters

> When you start services that accept parameters, you can specify these parameters at start up. You can start services on computers in the managed domain or managed subtree.

> **Note**
>
> You can start a service with parameters only through the Delegation and Configuration Console.

Specify a service startup type

> You can change the startup type of a service, such as requiring a manual startup.

Specify a service logon account

> You can change the service logon account to an account other than the current system account. You can specify the local system account, a specific user account, or a group Managed Service Account (gMSA) as the service logon account.

Restart a service

> You can restart a service running on a computer in the managed domain or managed subtree.

> To restart a service, you must have both the Stop a Service and Start a Service powers or you must be associated with a role that contains these powers, such as the Start Service role and Stop Service role.

Stop a service

> You can stop a service running on a computer in the managed domain or managed subtree.

Pause a service

> You can pause a service running on a computer in the managed domain or managed subtree. Whether a service can be paused or not depends on the type of service. For

example, you may not be able to pause a service that has dependent services.

Resume a paused service

You can resume a service that was paused on a computer in the managed domain or managed subtree.

1.7.4. Managing Printers and Print Jobs

To manage printers, you manage the print queues that service those printers. DRA enables you to pause or resume, start, modify, stop, and view resource printers and published printers. DRA also lets you modify the properties and priorities of print jobs. To add or delete a printer, use the native Windows tools.

A print server is a computer on which one or more logical printers are installed. A logical printer is defined on the computer that has the printer device driver. A logical printer includes the print driver, print queue, and ports for a printer. The print server associates logical printers with printer devices.

A connected printer is defined on the computers from which documents are selected for printing. A connected printer is a connection to a print share on the network. Therefore, you can manage printers and print jobs through the associated computers.

A published printer is a printer published in Active Directory. A published printer can be a network printer that is not directly connected to a server or it can be a printer hosted by a cluster server.

> **Note**
>
> You can manage printers and print jobs only through the Delegation and Configuration Console.

To learn more about managing printers and print tasks, see the following topics:

- Printer Management Tasks

- Print Job Management Tasks

- Published Printer Management Tasks

- Print Job Management Tasks for Published Printers

Printer Management Tasks

You can manage printers associated with computers in the managed domain or managed subtree. DRA lets you manage printers while managing other resources for that computer.

This section guides you through administering printers in the Delegation and Configuration console via the Account and Resource Management node. With the appropriate powers, you can perform various printer management tasks, such as stopping a printer.

Manage printer properties

You can manage properties for printers in the managed domain or managed subtree. DRA lets you manage printers while managing other resources for that computer.

Pause a printer

You can pause a printer associated with a computer in the managed domain or managed subtree. DRA lets you manage printers while managing other resources for that computer.

Resume a printer

You can resume a printer associated with a computer in the managed domain or managed subtree. DRA lets you manage printers while managing other resources for that computer.

Print Job Management Tasks

You can manage print jobs associated with printers in the managed domain or managed subtree. Because print jobs are associated with a printer, you can manage print jobs while managing the printer.

This section guides you through managing print jobs in the Account and Resource Management node of the Delegation and Configuration console. With the appropriate powers, you can perform various print job management tasks, such as canceling a print job.

Manage print job properties

You can modify print job properties as part of your printer management workflow. Because print jobs are associated with printers, you can modify the print job while managing the corresponding printer. The print job properties you can modify depend on the type of power you have. To modify print job properties, you must be able to access the corresponding printer and computer.

Pause a print job

You can pause a print job on a printer in a managed domain or managed subtree. To pause a print job, you must be able to access the corresponding printer and computer. Pausing a print job does not delete the print job from the print queue.

Resume a print job

You can resume a print job that was paused. To resume a print job, you must be able to access the corresponding printer and computer.

Restart a print job

You can restart a print job that was stopped. To restart a print job, you must be able to access the corresponding printer and computer.

Cancel a print job

You can cancel a print job that is in the printer queue. When you cancel a print job, DRA permanently deletes the print job from the printer queue. To cancel a print job, you must be able to access the corresponding printer and computer.

Published Printer Management Tasks

You can manage published printers in the managed domain or managed subtree. You can add or search for any printer that is published in the Active Directory or printers that are hosted by a cluster server.

This section guides you through administering published printers in the Account and Resource Management node. With the appropriate powers, you can perform various printer management tasks, such as stopping a printer.

Manage published printer properties

You can manage properties for published printers in the managed domain or managed subtree. DRA lets you manage published printers while managing other resources.

Refresh published printer information

You can refresh the published printer information in the managed domain or managed subtree. DRA lets you manage published printers while managing other resources.

Pause a published printer

You can pause a published printer in the managed domain or managed subtree. DRA lets you manage published printers while managing other resources.

Resume a published printer

You can resume a published printer that was paused in the managed domain or managed subtree. DRA lets you manage published printers while managing other resources.

Move a Published Printer

You can move a published printer available in one container in the managed domain to another container in the same domain. DRA lets you manage published printers while managing other resources.

Rename a published printer

You can rename a shared published printer in the Active Directory. DRA lets you manage published printers while managing other resources.

> **Note**
>
> Renaming a published printer in Active Directory does not change the resource printer share name or propagate the name change to the resource printer you want to manage. For example, if the resource printer name is Emerald and you rename the printer to Ruby in Active Directory, other users will see the printer name as Ruby, but the resource printer name will continue to be Emerald.

Print Job Management Tasks for Published Printers

You can manage printer jobs associated with published printers in the managed domain or managed subtree. Because print jobs are associated with a printer, you can manage print jobs while managing the published printer.

This section guides you through administering published printers in the Account and Resource Management node. With the appropriate powers, you can perform various print job management tasks, such as canceling a print job.

Manage print job properties

You can modify print job properties as part of your published printer management workflow. Because print jobs are associated with printers, you can modify the print job while managing the corresponding published printer. The print job properties you can modify depend on the type of power you have. To modify print job properties, you must be able to access the corresponding published printer.

Pause a print job

You can pause a print job on a published printer in a managed domain or managed subtree. To pause a print job, you must be able to access the corresponding published printer. Pausing a print job does not delete the print job from the print queue.

Resume a print job

You can resume a print job that was paused in a managed domain or managed subtree. To resume a print job, you must be able to access the corresponding published printer.

Restart a print job

You can restart a print job that was stopped in a managed domain or managed subtree. To restart a print job, you must be able to access the corresponding published printer.

Cancel a print job

You can cancel a print job that is in the printer queue in a managed domain or managed subtree. When you cancel a print job, DRA permanently deletes the print job from the printer queue. To cancel a print job, you must be able to access the corresponding published printer.

1.7.5. Managing Shares

A share is a way to make resources, such as files or printers, available to other users on the network. Each share has a share name that refers to a shared folder on the server. DRA manages the shares only on the computers in the managed domains. To successfully manage shares, the access account must have administrator permissions, such as being a member of the local Administrators group, on all computers where you want to manage resources. To assign these permissions, add the access account to the native Domain Admins group in the domain of the computer.

> **Note**
>
> You can manage shares only through the Delegation and Configuration Console.

Manage share properties

You can manage properties for shares in the managed domain or managed subtree. DRA lets you manage shares while managing other resources for that computer.

Create a share

You can create a share for a computer in the managed domain or managed subtree. You can also modify properties for this share.

Clone a share

You can clone a share for a computer in the managed domain or managed subtree. By cloning a share, you can quickly create shares based on other shares with similar properties. This flexibility lets you enforce consistent settings for all shares you create in a given domain.

When you clone a share, DRA populates the Clone Share Wizard with values from the selected share. You can also modify properties for the new share.

Delete a share

You can delete shares from computers in the managed domain or managed subtree.

1.7.6. Managing Connected Users

A session is established whenever a user connects to a particular resource on a remote computer. A connected user is a user connected to a shared resource on the network.

DRA manages connected users only on computers in managed domains. The access account must have administrator permissions, such as being a member of the local Administrators group, on all computers where you want to manage connected users. To assign these permissions, add the access account to the native Domain Admins group in the domain of the computer.

Disconnect a user

You can disconnect a connected user from a computer in the managed domain or managed subtree. You must be able to access the computer and this open session. Disconnecting a connected user ends the open session.

Refresh the list of connected users

To ensure you are viewing the latest information about open sessions on a computer, manually refresh the list of connected users. You must be able to access the computer and this open session.

1.7.7. Managing Devices

A device is any piece of equipment attached to a network, such as a computer, printer, modem, or any other peripheral equipment.

Although a device may be installed on your computer, Windows cannot recognize the device until you install and configure the appropriate driver. A device driver enables a specific piece of hardware to communicate with the operating system.

DRA enables you to configure and manage the devices only on the computers in the managed domains. The access account must have administrator permissions, such as being a member of the local Administrators group, on all computers where you want to manage devices. To assign these permissions, add the access account to the native Domain Admins group in the domain of the computer.

Manage device properties

> You can modify the properties of a device on a specific computer. Modifying the device properties for a device allows you to modify the startup type for a device.

Start a device

> You can start a device on a specific computer in the managed domain or managed subtree.

Stop a device

> You can stop a device on a specific computer in the managed domain or managed subtree.

1.7.8. Managing Event Logs

An event is an important system or application occurrence. The Windows operating system records information about events in event log files. There may be several event logs stored on each computer. Use the native Windows Event Viewer to view event logs. DRA manages the event logs only on the computers in the managed domains.

DRA records user-initiated operations in the log archive, a secure repository. You have the option to have DRA also record user-initiated operations in the Windows Event Log in addition to recording the information in the DRA log archive. For more information, see Understanding Dates and Times.

Event Log Types

Computers running Microsoft Windows record additional information in various logs. The logs are briefly described as follows:

Log Type	Description
ADAM	Records events logged by the ADAM repository.
Application	Records events logged by an application on the computer, such as a service startup or failure. For example, DRA stores events in the Application log.
Directory service	Records events related to domain controllers maintaining the security database.
File replication service	Records events related to file replication services provided by the operating system.
Security	Records events that include logon attempts, file and directory access, and security policy changes that are based on the audit policy options.
System	Records events logged by the Windows system components, such as the failure of a driver or services starting and stopping.

Event Log Management Tasks

When you install DRA, audit events are not logged in the Windows event log by default. You can enable this type of logging by modifying a registry key.

> **Caution**
>
> Be careful when editing your Windows Registry. If there is an error in your Registry, your computer may become nonfunctional. If an error occurs, you can restore the Registry to its state when you last successfully started your computer. For more information, see the Help for the Windows Registry Editor.

You can specify the maximum size of an event log file and what happens to an event log when it becomes full. The properties window also displays the name of the log, the log file path and filename, when the log was created, when it was last modified, and when it was last accessed. If you choose to back up the log file, DRA saves the event log with a unique file name in a standard location on the selected computer.

DRA lets you manage event logs while managing other resources for that computer. With the appropriate powers, you can perform various tasks such as changing event log properties.

Manage event log properties

You can modify event log properties for a specific computer.

View event log entries

You can view entries in a specific event log for a computer in the managed domain or managed subtree. In the Delegation and Configuration Console, you can view the event log file in the native Windows Event Viewer.

Clear the event Log

You can clear entries in a specific event log for a computer in the managed domain or managed subtree. You can also save the event log entries before clearing the log.

1.7.9. Managing Open Files

An open file is a connection to shared resources, such as files or pipes. A pipe is an inter-process communication mechanism that enables one process to communicate with another local or remote process.

DRA manages open files only on computers in the managed domain and managed subtree. Because open files are associated with a computer, you can manage open files while managing other resources for that computer. For example, you may want to close open files when you shut down a system or install a new device or service. You can also monitor which files users access most often, helping you better assess file security.

> **Note**
>
> You can manage open files only through the Delegation and Configuration Console.

Close a file

You can close open files from resources on the network. It is a good idea to notify users when you intend to close open files. They may need time to save their data. To close an open file, you must be able to access the corresponding computer.

Refresh the list of open files

To ensure you are viewing the latest information about open sessions on a computer, manually refresh the list of connected users. To refresh the open file list, you must be able to access the corresponding computer.

1.8. Managing the Recycle Bin

The Recycle Bin provides a safety net by allowing you to delete user accounts, groups, contacts, and computer accounts on a temporary basis. You can then restore these objects to their original state with all data, such as SIDs, ACLs, and group memberships intact or permanently delete these objects. This flexibility provides a safer way to manage user accounts, groups, contacts, and computer accounts. You can use the search option to search for required objects. For information, see Searching for Objects.

Restore an object from the Recycle Bin

> You can restore deleted objects back to the containers from which you deleted the objects. DRA restores these objects to their original state with all data, such as SIDs, ACLs, and group memberships intact. An object can be a user account, group, contact, dynamic group, resource mailbox, dynamic distribution group, or computer account.

Restore all Objects

> You can restore all objects from the Recycle Bin for a managed domain. You can restore objects from the Recycle Bin for a specific domain or across all managed domains. To restore objects from a Recycle Bin for a specific domain, the Recycle Bin must be enabled for that domain.

Delete an object from the Recycle Bin

> You can permanently delete objects from the Recycle Bin for a managed domain. Once you delete an object from the Recycle Bin, you cannot restore the object. An object can be a user account, group, contact, dynamic group, resource mailbox, dynamic distribution group, or computer account.

Empty the Recycle Bin

> You can empty the Recycle Bin for a managed domain. Emptying the Recycle Bin permanently deletes any objects currently in the Recycle Bin. You can empty the Recycle Bin for a specific domain or across all managed domains. To empty a Recycle Bin for a specific domain, the Recycle Bin must be enabled for that domain. Once you empty the Recycle Bin, you cannot restore the deleted objects.

opentext™

© Copyright 2025 Open Text

For more info, visit https://docs.microfocus.com